MONTREAL – At-Large Policy Session: EPDP phase 2
Sunday, November 3, 2019 – 10:30 to 12:00 EDT
ICANN66 | Montréal, Canada

ALAN GREENBERG: For those who don't know me, I'm Alan Greenberg. I am one of the two ALAC-appointed members of the Expedited PDP. And by the way, if you call it the EP-DP, we kick you out of the room. It's an E-PDP. I only respond to people who speak into a microphone, and I'm not giving you the microphone right now. And my partner in crime is Hadia El Miniawi. We also have two alternates: Holly Raiche and Bastian Goslings. Can we have the slides up, please?

The agenda is relatively simple. We'll talk a little bit about the background of how we got here EPDP Phase 1, which ran from middle-to-late last year to the beginning of this year, 2019. We are now in Phase 2. This is unusual in a PDP. Normally, a PDP has a subject, a set of reports, a final report and then it disappears. We have two discrete sections, each of which will have had or will have reports, recommendations, Board approval, and then go on to the next one. And heaven help us, maybe we'll have a phase three.

We'll talk a little bit about Phase 1, Phase 2. The SSAD the standardized disclosure system that we are talking about -- which may or may not be possible in questions -- it's a very short presentation, we only have 10 slides, and we're not going to go into a lot of depth, and hopefully we'll have a lot of opportunity for questions. Next slide, please.

Note: The following is the output resulting from transcribing an audio file into a word/text document. Although the transcription is largely accurate, in some cases may be incomplete or inaccurate due to inaudible passages and grammatical corrections. It is posted as an aid to the original audio file, but should not be treated as an authoritative record.
Alright, the background. There's been privacy legislation in Europe, and many other places, for a good deal of time. ICANN has been, at some level, conscious of it. And the focus with ICANN privacy legislation has very much been on WHOIS. Because although there are lots of aspects of ICANN where we have to worry about privacy -- and if you’re paying attention, you’re seeing lots of changes in ICANN and lots of disclaimers and lots of places you have to take off a box related to privacy -- but WHOIS has been a particular one because the requirements of WHOIS, and in fact, going back to ICANN being created, one of the mandates of ICANN is to have a WHOIS which makes public information about who the registrants are and how to contact them. Very soon after that became a practice, privacy and proxy providers were invented to hide things. Often, that is an added value cost item, but nevertheless, as a service available to many people.

The European general data protection regulation went into place in 2016, which was a modification of its predecessor laws and regulations. The difference here is, with a two-year delay, there were very significant penalties. Although penalties are proportionate, depending on what the infraction is, they can be as high as four percent of global income, not profit, income. That’s the profit margin in many companies. So this is serious stuff. And suddenly, it became a real issue that ICANN had to worry about, because it’s contracted parties, particularly those in Europe, have a vested interest, a financial interest, in not having penalties.
To address the issue, the Board adopted something called a temporary specification. That name is a curious one, but it follows the form of the contracts ICANN has. If you look at the contracts with contracted parties, registrar’s and registries, there's a base contract and then there's a number of addendums, which are called specifications, which govern certain specific details associated with the contract. And this was a specification to be added onto the contract, but it was to be temporary only, thus called the temporary specification. And it was modifying the contracts to be reasonably compliant with GDPR. And it allowed contracted parties to redact information that otherwise they might have had to display.

And there’s a whole bunch of other details associated with it. However, because this is temporary specification, the contracts with registrars -- with registries, rather -- allow a temporary specification. It can be in effect for three months only, and is renewable, but renewable to a total length of only one year. So, essentially, it says the Board can enact policy in an emergency when the normal processes can't work that fast, but it only can last year. So the Expedited PDP was chartered with saying, "Come up with a plan to have a real policy, to replace the temporary policy within the one-year period." And to a large extent, we did it.

There was a phase in period, we provided the policy and enough time for the Board to approve it by the right dates. But, that wouldn't give the contracted parties enough time to implement it. We’re talking about writing code, in many cases. The policy also said that the
contracted parties have about a year, a little bit less, in which to implement it.

And in the interim, we are adopting a policy comparable to the temporary spec. It's not the temporary spec anymore, it's a new policy, but it has the same words as the temporary spec. So that gave the transition period, and we're still in that transition period. It ends, I believe, on the 29th of February 2020, by which time, all contracted parties have to go along with the Phase 1 policy. And that's where we are right now.

There were a few leftover things that we couldn't fix, that we couldn't come to closure on. Those are rolled over into Phase 2. The main part of Phase 2 is saying, now that the registrars and registries are compliant with GDPR and we are redacting a huge amount of information, GDPR allows that information -- the redacted information -- to be given out to certain parties under certain conditions.

Our challenge now is, can we build a system to do this, or do we have to do what we're currently doing right now? If you want information, you go to the particular registrar, registry and they do it all on their own. There's no consistency. There's no uniformity. And in some cases, there's no answers. We'll talk a little bit about that as we go forward, but that's where we are right now. And I'm going to turn it over to Hadia to do an overview of the Phase 1 implementation. Thank you. But if I left anything out of what I said in my intro, please do it first.
HADIA EL MINIAWI: Thank you, Alan. No, actually, you did not leave out anything. So, as Alan said, it was necessary for the community to come up with a consensus policy that would eventually replace the temp spec. And to do so, the expedited policy development process for gTLD team was formed. It was adopted by the GNSO council in March two thousand -- okay -- So, the EPDP Phase 1 was able to come up with a consensus policy, which was actually adopted by the GNSO council in March of 2019. And then, the Board passed a resolution that adopted 27 out of the 29 recommendations.

So, the Expedited Positive Development Process came up with 29 recommendations, two of which were not adopted. The ones that were not adopted was recommendation 1, purpose 2, which spoke about the ICANN purpose to maintain the stability and resiliency of the DNS. However, the reason the Board did not adopt this recommendation is that part of it was seen as an activity rather than a purpose. And in all cases, this was a placeholder that was going to be addressed during Phase 2.

The other recommendation that was not adopted by the Board was one with regard to the organization field, where there was an option to either delete or redact the organization field if request to the data subjects were sent to affirm the data that was in that field and there were no responses. And the Board thought that the deletion of such information could have a negative impact on the data subject as it might lead to an organization losing its right to the name.
So as we said, we recommended a new gTLD registration policy. We recommended adopting an interim policy, based on the temp spec. And the effective date foreseen for the Phase 1 policy is 29th of February 2020. That doesn't mean that registrars cannot, or registries cannot, actually implement before that date, but that's the deadline for all to be in compliance with new policy. Could we have the next slide please?

So, what we addressed in Phase 1 were the purposes for the processing of the data, the legal basis for the processing of the data, which data should be collected, for how long should the data be retained, and which data elements could actually be disclosed in case there is a legitimate request that has been approved. What we did not determine, who are the controllers -- who's the controller, who's the processor. And also, one issue that rose, that there's evidence that the policy that we developed might not be working in some current cases. But this is because, I think, the whole work of the EPDP Phase 1 and two, is not complete yet.

One important aspect to look at here is the reason it was necessary to have such policies. Of course, its compliance with GDPR, but also, it gives data subject some more transparency and the ability to have control over their data, because they're able to know which data is collected, for which purposes, by whom, who is it held by, and the circumstances under which this data could actually be shared with third parties. So, this actually enhances the privacy of the data subjects.
And what we're looking for in Phase 2 to actually further enhance the protection of the personal data of the data subjects, and also to allow for the legitimate requests for data to be able to go through and have accurate data that they could actually use for their legitimate interests. And that lies, really, within the interests of the Internet end users, because if we talk about the security of the DNS and the security of the websites and the stability of the Internet, it directly impacts end users. And I think this is where we, as ALAC, come from when we participate in this policy development process. We are focused, definitely, on the rights of the data subjects, but we are looking also for the rights of the end users as well. So I'll let Alan continue.

ALAN GREENBERG: One of the interesting things that just came to light in the last day or so, and that's the illusion of the last item. As I said, we've developed a policy that is now in place, on an interim basis, for how someone who believes they have legitimate access to redacted data, can ask for it. And it's been implemented. What recently came to light is, there was a situation where someone had a complaint about a website in Europe, and they made a complaint to their own data protection office.

That data protection office looked at it and said, "Yes, this seems to be problematic. But to further address it, we need to know who the registrant is." And they made a request, under the current practice, to the registrar to release the information. Now, as the data protection officer, they looked at their motivation and what the law says about under what conditions is information allowed to be released, and they
believed they have a valid request. The registrar said no. So they have now filed a complaint with ICANN Compliance.

So, bottom line is, there are currently implementations of how people are interpreting the policy we developed, that not only Hadia and I may disagree and say people [inaudible], but the data protection officers are saying we’re not in compliance by releasing information where we should. We were also told they have another 40 complaints on their desk that they’re waiting to file with ICANN Compliance. I just heard the story once, and I may have some of the details wrong, but I believe that is pretty close to the gist of it.

So clearly, we have built a structure and it’s not working, even according to the data protection officers whose job is to map privacy, but when they feel the privacy information should be revealed. We are being overzealous. We are overzealous in other ways because data protection law applies only to natural persons. We have given registrars and registries the right to apply it to legal persons, to anyone. It applies only in certain physical areas, but we have given the registrars and registries the right to, essentially, ignore geographic areas and apply it universally.

Now, this was hit home by one of the registry representatives -- is from Donuts. Now, registries don’t get a lot of requests, but remember, new gTLDs are thick registries, so the registries do have the information. And he is the data protection officer for Donuts. So he gets all of the requests. He doesn’t get a lot. You know, perhaps 70 a year, or something like that, is what the record is so far. But he went through
his process in evaluating these. And a key part of the process is, a balancing act has to be done to look at the competing needs of the benefits of releasing the information to the requester, versus the protection of the registrant -- the privacy of the registrant.

At the time he gave that report, which is a month or so ago, of the hundred reports he was summarizing -- the requests he was summarizing -- he has never had to exercise a balancing test. Because of the requests, which ended up being valid and had all of the parts filled in and weren’t empty forms, all of them were ones that GDPR did not apply to. They were natural persons, or the geographic area was such that there was no reason to redact the information. So although the balancing test has been the subject of a huge amount of discussion, in his case, he never had to do one. So, it’s interesting environment. Okay, next slide please.

The issues the ALAC had with Phase 1, and we went on record with these, is legal versus natural, that we believe it was over-applied, geographic differentiation -- and some people in At-Large differ on that and they feel we should apply our rules uniformly to everybody, but we did have ALAC consensus to identify this as an issue -- the organization field was one that we had some concerns with, although we were willing to accept it until the Board pointed out that we really shouldn’t. And we are still in an issue where the registrars are saying they want the option of deleting information.

There is now some implementation guidance which may say the register can delete the information but has to keep it in their back
pocket, so if there's ever a question of ownership, they could retrieve it. But it would not be provided, even on an access request. And as I said, the indications that the policy is not even working, even in its current implementation -- and that's problematic going forward.

The next slide is beginning of the Phase 2 work, and I'll turn it back over to Hadia, unless Hadia has anything to add on this point. I'm holding all questions. We will do with the report -- the presentation is over halfway through right now, so we'll group all questions at the end. Hadia.

HADIA EL MINIAWI: Thank you, Alan. So here we are. We started EPDP Phase 2. And mainly, EPDP Phase 2 is to address who can have access to the data, under what circumstances that data could be disclosed, the data fields to be disclosed with regard to each request. And remember, each request corresponds to a purpose, and depending on the purpose, the data fields are determined. The means through which a user can submit a request to the system and the means through which he could actually receive a response, and in case that response is that he can have access to the data, what are the means of disclosure.

And in doing so, first, to determine who can have access to the system, we considered some possible use cases. Different stakeholder groups presented possible use cases. So for example, the ALAC presented two use cases. One of them presents when an Internet end user could actually request the data of a domain name, and the other
represented the consumer protection agencies. Similarly, other stakeholder groups represented real life use cases. And that helped us to determine the users of the system.

When we talk about the means of submitting a request and the means of the disclosure, we're talking here about a system, a system through which the users or the requesters could actually submit a request and that request would be evaluated. And depending on the evaluation, a decision is made to whether data is disclosed or not, which data fields are to be disclosed. EPDP Phase 2 also talks about the issues differed from Phase 1. Like legal versus natural, that's an example. And that's an issue that we were talking about yesterday. We were setting a study in that regard, and based on the result of this study, further consideration will be taken. If we could have the next slide please.

In looking at the means of submitting a request and the means of receiving a disclosure, again, we look at the data subject. And we think important elements for the data subject to have control over the data. In Phase 1 we looked at which data should be collected. And the data subject now, which data is held, by whom, the retention periods, and under what circumstances that data could be disclosed.

In EPDP two, and looking at the standardized access and disclosure system, we want to take this one step further. And by having a standard system that can actually respond to the requests of the requesters, we have a more predictable system through which the user can know exactly under which circumstances the data could be shared with others.
And that's why it's important to have a standardized system. If we currently have more than 2,500 registrars, and each one of them is going to apply his own terms when they receive a request for a domain name disclosure, then this would provide inconsistency, and also, provide an unpredictable system. So we were looking for a transparent, predictable system.

On the other hand, also, we were looking at the requesters, and again, trying to ensure that there is a system in place that is consistent through which the requesters can go through and get answers to their requests. And as Alan mentioned, as we currently stand, even though we develop EPDP Phase 1, legitimate requesters with lawful basis do not get their requests. And you have the DPA saying that, and not like stakeholder groups within ICANN, saying that.

So hopefully, in Phase 2, we are able to address this, we are able to come up with a standardized access disclosure system, and maybe even a unified access model. Because you can develop the standards and have a standardized access disclosure system, but still you have this distributed system, because all the data lies, as you all know, with the registries and registrars. So, though we could have the standards, but having a non-uniform distributed system also is not the optimum solution.

Because again, it will be up to the registry or registrar to apply those standards, and how to apply those standards might differ from one to another. So, I would say our ultimate goal is to have a unified access model. How this model looks like, we don't know yet. And whether it
would be really possible or not, we don't know yet. But at least, we are looking for a standardized system. And I would leave Alan to continue. Thank you.

ALAN GREENBERG:

Thank you. Next slide. The title of this slide needs an explanation, for those who are not native English speakers. "The elephant in the room" is an expression, in English, which refers to something that everyone knows about, you can't ignore it, just as you can't ignore an elephant who might be in this room, but you don't talk about it or you ignore the issue because it's too difficult, or something like that. The elephant in the room here is, if we are going to have a standardized access method with uniformity, how do you do that?

You might remember from Phase 1, we said we haven't quite determined who the controllers are. Well, the controller is a technical term in data protection law, which basically says, this is the entity that controls things. If the controller releases the information and a complaint is made, there may be a penalty imposed upon the controller. There may also be third party legal action against the controller, but we're just talking about the penalties imposed by the data protection authorities.

So in a simple model of a standardized model, ICANN would run this, ICANN would make a decision on whether to release the data. And if there was a problem, the registrar, registry would pay the penalty. Well, they're not going to accept that. Yeah, we're not going to talk
about paying penalties of four percent of their gross income, potentially, in the worst case, where they didn't even make the decision.

If you don't have that kind of thing, in at least some cases, then you're, number one, reverting to completely manual processes. Manual processes are not practical for many types of requests. If someone has a trademark -- take a simple random trademark, like Facebook. There are a lot of people who look at the money that Facebook draws in saying, "Can we get a part of it? Legal or not legal."

Therefore, people register domain names that look like Facebook. They may look exactly like Facebook, using other scripts. You may use other techniques to try to convince people you are Facebook. No matter what you think about Facebook, it doesn't really matter because you could apply some other name of some company you don't dislike. But if you're protecting those kind of trademarks, you may well have thousands of hits, thousands of entries that are trying to use your thing.

Cybersecurity is another one. We know, for instance, that the people who run botnets and things might register 1,000 or 10,000 domain names in a single pass. There may be a lot of information you want to get if you're trying to fight these kind of things. So, we're talking about potentially high volumes, we're talking about the need to address these things quickly, that we can't put you in a queue and get back to you three months later. That's not going to quite meet meet some of
the needs. So an automated system, at least, partially automated. There's always going to be decisions that have to be made manually.

But the question is, do you always have to make them? So the question is, can a centralized authority make these decisions and assume the liability. Now, remember we talked about controllers, there's a general presumption right now that both ICANN and -- because we set the policies, we can't avoid being a controller, we set the rules -- but the registrars and registries also may be controllers. Whether we're joint controllers or independent controllers, not clear at this point.

The question is, can ICANN make the decisions and assume the liability? Is ICANN willing to assume it? There's an indication, at this point, they are. And are they willing -- will that be allowed under data protection law? So we are looking at how to build a system, but we're not sure the system is legal or will be accepted.

And currently that's being tested. ICANN has posed a number of questions to the European Data Protection Board. We hope to get some answers that might give us some guidance, but at the same time, we're trying to build the system making the assumption that we may be allowed to do some of this or all of this. But we're not quite sure.

It's quite clear that, if you're looking at cybersecurity requests or, for that matter, intellectual property requests, they're going to follow certain patterns. And if you looked at 100 of them and they're all
identical, except for the domain name and the, perhaps, proof that you own the trademark, we can build computers to recognize those patterns also. And it's conceivable that we may find that making these kind of decisions is something that can be done in an automated way for some classes, requests, and perhaps, the high-volume requests. And that's what we're looking for.

There's always going to be some that are subjective, and decisions will have to be made by humans. How do you process those? Can we accept those all in a same unified way so we log them, we track them? And maybe some bounce all the way down to the contracted party. Remember, contracted parties, registrars, not only have the information WHOIS, they also have the information about their clients. So they have a lot more information about who the registrant is that is not part of WHOIS. That information is never going to be held outside of the registrar.

So, there's always going to be a significant number that go down to that level. The question is, can we skim the top off and make it easier, and can we make sure we have uniform reporting and tracking? And that's the real crux of an SSAD. And at this point, we are hoping we may get an answer, by January or so, from the Data Protection Board. We hope it's going on their agenda in the December meeting. And come January, we may be in a better position to actually know that what we want to do is possible, potentially legal, or it's off the table all together.
But there's a lot of sub questions that also come up. One of the questions that comes up is, if you, as a legal person -- a company -- put in your contact information as joanna at icann dot org, and that information is released and you complain, who do you complain to? Do you complain to the person who released the data? Or do you complain to the registrant, the legal entity, that made the registration that put your data in?

Well, there's no definitive answer. Different legal authorities in Europe, some view at one way, some view with the other way. If we had uniformity and knowledge of that, that would help things like, if we can recognize a legal entity, then we know we can give up the information, even if there's personal information in their registration entry. Because, yes, someone is going to be at blame, but it's not us. It's whoever put it in. And as I said, different legal entities in Europe have viewed one way or the other. So, it's a challenge. Next slide.

All right, let's recap why we are interested in all this. End users need to trust the Internet. We have currently, last number as of July, I believe, 4.33 billion users. And trust is important. There's lots and lots of fraud, phishing, spam, all sorts of things that use domain names heavily. One of the interesting things that came out in our discussions is, a typical usage is if you are using or distributing phishing or malware, you will often break into some innocent person's website, add a page to it, a directory to it, and do your phishing pointing to their website. The easy way to address phishing is take down the website. You go to the registrar or the web host and say, "Gone".
But now you're taking down the real one that the owner had, maybe the local fishing club -- well, not fishing, sorry, bad example -- the local kennel club. And what cyber people used to do is contact the registrant and say, someone's broken into your site. Now we can't find out who the restaurant is. So it's really interesting that these things sometimes work backwards from the way we want to do it. We're hurting the person we think we're protecting.

But it's really challenging. Consumer Protection need access to this kind of information. Remediation is often really time critical. And the bottom line is, people are not going to trust the Internet if they can't click on a link and presume it's going to work. We had the same discussion on DNS abuse. If you can't believe it's going to work, you're not going to put your faith in it. And yes, you'll use it because people are not going to stop using the Internet, but it's not the system we want. Hadia, anything to add on that one?

HADIA EL MINIAWI: No.

ALAN GREENBERG: Then we'll open it up for questions. And I hope someone's been keeping track of the queue.

GREG AARON: The queue, at this point, is Holly, Olivier, Tijani, Umberto and Seun. So, we'll begin with Holly. And just to note, we have about a half an
hour, so we should have plenty of time, but let's try to keep things brief.

HOLLY RAICHE: It's really just a minor question, but I thought you mentioned that there may be some question whether consumer protection agencies would be amongst those people who would have access to the data.

ALAN GREENBERG: I said consumer protection is an important area. We are talking about, users of the SSAD will have to be accredited. It simply means we can identify them, and we may know something about them. I would suspect that government consumer protection organizations, and conceivably, private ones, are groups that we could accredit and have some level of trust in that they will obey the rules.

Remember, if information is released to you, it's released under certain stringent conditions, that you can only use it for the reasons you asked for it. You have to destroy it when you no longer need it. There's a whole bunch of if, but's and and's. I like to assume, and certainly our friends on the GAC would like to assume, that consumer protection is going to be one of the groups that end up having access. You're not going to get me to give you a guarantee.

HADIA EL MINIAWI: Just want to add one thing, maybe we did not mention throughout the presentation, that we're what we're looking into right now is actually a
system based on accreditation. So we are looking into a system where every user to the system needs to be accredited. So whether it's an entity or it's an individual requester, they will need to be accredited in order to be able to use the system. However, being accredited does not mean that you will get access to the data or get the data. Just to use the system, you'll need to be accredited.

GREG AARON: Tijani, do you have a direct response on that?

TIJANI BEN JEMAA: I have a point of order. I propose that Alan and Hadia collect all the questions and answer at the end. Otherwise, we will not have the time to have the floor.

GREG AARON: It's up to you, Maureen. But I think we have a half an hour or so. I think we're okay, actually.

MAUREEN HILYARD: Yeah, I think we're okay.

GREG AARON: Olivier.
OLIVIER CREPIN-LEBLOND: Thank you very much, Mr. Chair. I have two questions. Very short one. The first one was to do with some discussions that were taking place on the EPDP mailing list. And I do lurk from time to time, seeing the flood of emails in there. And there was some vehement opposition towards any kind of automation in the system, which to me, looked as though -- well, basically killing the system altogether, as you very rightfully explained. Does one require full consensus in the group for automation, or at least parts of it, to work? Or is this -- might we end up with a status quo --

ALAN GREENBERG: Ask your second question and then we'll answer.

OLIVIER CREPIN-LEBLOND: Okay. And then the second one was to do with -- with me forgetting the second one. So I'll go back in the queue in a second.

ALAN GREENBERG: Number one, there are people in the group who have very different positions. There are those who believe that we are never going to be able to build a system with any level of automation assistance to tell you, yes, this person is accredited. But there will always be a human being making the final decision in every single case. There are others who believe,

I gave my example of, once you've looked at 1,000 requests and they're all similar and you've said yes, do we really have to look at the
next million by hand? The definition of insanity is doing the same thing over again and expecting different answers. So, I'll leave it at that. Do we need full consensus? We are striving for full consensus. Ultimately, the PDP, like every PDP, has rules about how do you judge consensus, and it's up to the Chair, and then another set of processes, but we're certainly trying to find compromise which everyone can accept.

OLIVIER CREPIN-LEBLOND: Thank you, Alan. I remembered my second question, which is very short. And it's to do with the case use scenarios that the community worked on, and some that we proposed as being for end users being able to consult the information. What happened with the case use scenarios at the end? Were they helpful? Were they used? Or was it just seen as an exercise that just ended up down the drain?

HADIA EL MINIAWI: Actually, I would say they were useful. And in particular, our use cases, we were able to present a real case so that -- we're not talking about curious users out there trying to get who registered this domain name. So yes, I would say they were useful. And I'm not sure if the use cases will be, at some point, included somewhere. But yeah, they were useful. And that's how we ended up with the user groups, and also ended up with lots of many other recommendations. So with regard to the safeguards and what the requester should provide in the request and how the responses should look like --
ALAN GREENBERG: I believe the decision was, there clearly will form part of the body of our work but will not be in the final report, because they were not designed to be exhaustive. And it’s somewhere misleading in some cases.

GREG AARON: Tijani.

TIJANI BEN JEMAA: Thank you very much. Alan, I have difficulty to understand your example of a DPO accepting to disclose non-public data while the registrar refuse. Because the GDPR says that the party who are collecting, processing, transferring, etc., data, are the one who appoint the DPO in their enterprise. The DPO will be part of the registrar, so the registrar has the data, the registrar collects the data, the registrar processes the data. So I don’t understand how, first question.

ALAN GREENBERG: The entity that requests the data [inaudible] was not the data protection officer in the registrar, it was data protection authority in the country.
TIJANI BEN JEMAA: So, it is not the officer? The data protection officer and the GDPR is appointed inside the entity who is collecting --

ALAN GREENBERG: I apologize if I used the wrong word. I was referring to a request from the Data Protection Authority in the country. And the ones who interpret the law and decided that this was a reasonable request, but the registrar did not agree.

OLIVIER CREPIN-LEBLOND: I think Alan used the word data protection office, but it may have been a little hard to hear.

TIJANI BEN JEMAA: Okay. Thank you. And second question, ICANN, being the data controller. Very important question, very difficult to address. Because the data are not in the hand of, of ICANN. They are in the hand of the registrar. So ICANN will be the sanctions, being the controller while they don't have the data. And I think that this will be a very difficult issue. And another point, very important, also regarding the controller. Sorry, I forget.

ALAN GREENBERG: There is no question that ICANN is a controller. We set the policies. We sit in these rooms and write the policies that govern how the -- There's absolutely no way we cannot be a controller. Are we the sole
controller, a joint controller, two independent controllers? All good questions that has not been addressed.

GREG AARON: Humberto?

HUMBERTO CARRASCO: Thank you very much. I'm going to speak in Spanish.

HADIA EL MINIAWI: It's just a comment that you should bear in mind when we talk about responsibilities, there are different responsibilities for different actions and different activities. So, if we talk about liability with regard to disclosure, that would differ if the disclosure is done through a gateway, whether it's ICANN or another entity or whether it's done through the registrars.

When we talk about the decision making also, the responsibility and liability will lie with those responsible for the activity. So, when we talk about moving the liability, for example, from the contracted parties to, for example, ICANN or to another entity, we are not talking about moving all the liability. We are talking about the responsibility of certain actions or certain activities. But they are still liable for other related data processing actions. Thank you.
ALAN GREENBERG: Just to be clear, when we're talking about removing liability, that's a shorthand for some relatively complex legal terms which don't mention those words.

HUMBERTO CARRASCO: I would like to thank you for the presentation. I think it's a very good summary of the issue. My first question was related to the liability, and it's crystal clear that ICANN, by setting the policies, is somehow liable. The liability has to be defined in specific cases. It's different from what happens to contracted parties, but it's clear.

I believe that ICANN is liable to some extent, but I am sort of worried, or fear, that all this work depends on the consultations or inquires ICANN submits to European Commission. We have to wait for their response to see what decision we're going to take up. So, we are working on the assumption. And depending on the answer we get, we will have to change that path or the alternatives we are choosing. And this creates a lot of uncertainty, all kinds of uncertainties. We have spent resources and time, we may have a caucus with experts from different cultures, because the opinion of a US lawyer will be different from the opinion of a EU lawyer.

My question is, I would like to know whether you have taken all this into account. But I'm concerned that we may come to the end of the year and we will have no certainties about the actual result, what path we will have to follow depending on the EU Commission answer. This is the point.
ALAN GREENBERG: We're going to get an answer which will help us. We might not. We might get an answer which rules out certain things, but doesn't say other things are okay. But working completely blindly, that's not very useful either. We certainly don't want to put a big thing in place, build a complex system, and then be told, "Oh, that's not legal." So we're hoping that isn't the case.

The way the data protection officers and the European Data Protection Board normally work though, is not to give prior answers, but to judge very often after the fact. They do issue rulings and do issue guidance papers. So, we're hoping. Is it a mess? Yes. Is there a simple path through it? No. Do we have any choice but to try to move forward? Yes -- no, we don't have any choice.

HADIA EL MINIAWI: So again, you rightfully said that the question sent out by ICANN Org to the European Data Protection Board, with regard to a unified access model, will actually inform a lot of our policy decisions. Having said so, if they come back and say, this is not legally possible, then this is something that we will discard. And when, trying to come up with a policy, those are things that we are not going to do. So that's very helpful.

On the other hand, if they say that this is legal that doesn't mean that this is actually the policy that we are going to do, but to a great extent, it does make sense that we adopt it. But then again, it informs our
policy decisions, but it's not necessary what we are actually going to do or follow. So, we are waiting for the answers. And yes, it might put things off the table and it might bring things on the table. Thank you.

ALAN GREENBERG: As pointed out, the group is divided. There are those people who feel don't care whether the Data Protection Board says, "It's okay, we don't want to do it."

GREG AARON: Seun, you're next.

ALAN GREENBERG: We have 20 minutes left, slightly under.

SEUN OJEDEJI: A couple of my questions have been answered. This is just a point of information question. So this work of the group, I would say, has been looking at the GDPR in detail. And I think as far as Internet is concerned, this is probably one of the groups that has been looking at GDPR in detail, globally. So I just wanted to confirm, as much as GDPR is very good, it's not perfect.

I wish that they have written something differently in the context of the GDPR itself. So, while I think that it may be out of scope for the EPDP, in terms of what they are doing, are you getting some engagement from the European Commission, or is there a separate
group within ICANN that is actually looking at possible improvement to the GDPR? And would that be within scope of ICANN?

Because personally, there are some things that I see in GDPR that I'm like, "Were they really considering the Internet when they were writing this stuff up?" So I wanted to confirm whether there is really that window that we are not losing, because I think that a lot of work has been done in this group, and I think if it contributes back to improving the GDPR, it will also be a good thing. Thank you.

ALAN GREENBERG: I have heard people who are in positions who understand these things, say the European Commission, when drafting this legislation, had no clue how WHOIS worked, or the fact that it was not a single database held by ICANN. I have heard other people in similar positions of authority said, "Of course, they understood at all." So take that as a basis. There is work undergoing in the European Commission right now to look at revisions, probably in the 2025-‘26 time frame. So we're not going to solve our problems.

Are we working with those people? Well, we have some European Commission people on the EPDP. I suspect they may be involved in those activities, although I've never asked them. I don't think anyone at ICANN is working with them right now in an explicit way. But there are discussions going on, and revisions, obviously. Any law like this is going to have revisions.
SEUN OJEDEJI: Just a quick follow on. May I? Okay. I really suggest that a representative kind of consider suggesting this to ICANN. They should probably keep in close in that process, and hopefully, that would also improve the GDPR ’20 -- whenever they finally develop the new draft. Thanks.

ALAN GREENBERG: I would suspect the cybersecurity people in the countries within Europe who are struggling to survive, are the ones who should be advising their own government of the kind of changes that are necessary.

SEUN OJEDEJI: Well, we are [inaudible] anyway. So, if you don’t want to be involved in reviewing it, so be it. We [inaudible].

GREG AARON: Matthias.

MATTHIAS HUDOBNIK: Hadia and Alan, thank you very much for the brief update. I have two questions. The first question, I would be curious to hear from you, from a realistic point of view, do you think that there is a chance to have a unified access model at the end? This would be my first question.
And the second one, regarding the accreditation model, is there a federal model already? Because there's one from PricewaterhouseCoopers, there's one from the WIPO. Law enforcement has also some kind of accreditation, at least, a proposed something. So, is there already something, some trends going on, where you can say this would be like going in this or that direction? Thank you.

HADIA EL MINIAWI: Okay. Thank you for the question. Your first was?

MATTHIAS HUDOBNIK: My first question was regarding a unified access model.

HADIA EL MINIAWI: Okay, yeah, if it's possible or not. So, my personal thinking, that if it's legally permissible to have a unified access model as the one developed by the technical study group, and the one put forward to the European Data Protection Board, if it turns out that it is legally permissible, yes. There is a very good chance that it can be actually adopted and implemented.

And let me tell you, the first ones that would actually be pushing for it, if it is actually legally permissible to have it, will be the contracted parties. Because it relieves them from being responsible about the disclosure of the data. They remain responsible about the other aspects of the processing, but that part -- so, if it turns out that it
actually does sell. Again, we don't know. So it depends on the answers that we get from the European Data Protection Board. If it turns out that that says system removes their responsibility or liability with regard to the disclosure of the -- if it doesn't, then no, I do not see such a system like the model.

Because you could have different models of the unified access model and different models for standardized access system. And so, you could have a standardized access system with distributed -- centralized in the sense that you have one unique system through which you receive the request, and maybe also disclose the answer, but distribute it in the sense that you have the individual contracted parties making the decision of the disclosure. So, there are many possible models.

The European Data Protection Board has been asked about one specific model, but there are other many alternatives. So definitely, we will have I think again a standardized system for access and disclosure. How this system looks like, it could have different types of models. We don't know yet. And then the second?

MATTHIAS HUDOBNIK: The second question was about the accreditation models.

HADIA EL MINIAWI: Okay, so what we've been actually trying to do is to put the policies for an accreditation model to serve the standardized system for access
and disclosure. So we haven’t been talking about which other entities could actually be part of this model, or which other entities could help in this regard. So we were putting like, broad principles, like you will need to have an accreditation authority. Who that accreditation authority is, we don't know yet, but we think it could be ICANN.

And then, accreditation authority will accredit one entity to actually accredit the users. It could have accredit many, but then again, it could be one. Again, they could contract other entities to do the accreditation part. But we are setting the broad lines, like, who should be accredited, for example. So again, as I said before, we are looking that everyone who uses the system should be accredited. And that would be either a user or an entity. So that’s it.

ALAN GREENBERG: But the bottom line is, we will have a system. To what extent it will be automated or not, is questionable. We will have accreditation. Exactly how it will work, we're working on it. We're really starting to get short of time, so I ask the questions and the answer to be really brief.

GREG AARON; We have five in the queue and 10 minutes. I’m putting on a two-minute timer, just to try to keep questions and answers within those. Next, we have Javier followed by Joanna, Bartlett, Tijani and Dev.
JAVIER RUA-JOVET: Thank you, Greg. Thanks Alan, Hadia. Quick question, not on substantive issues, but more on process. Does an Expedited PDP type of process -- is that expected to inform future processes like PDP 3.0 thinking, or is this really an extraordinary type of measure?

ALAN GREENBERG: The Expedited PDP is one of the multiple policy development processes that were developed a few years ago. This is the first time it's being used. Despite what some people think, it is not necessarily one that will only be used in cataclysmic things and with specific structures. One of the reasons it was designed is, what if something is important to be done but it's not really controversial? Can we bypass some of the reports and some of the processes which are required in a real PDP, which lengthen it into at least a year and probably a year and a half?

So, there is no issues report necessary, because it's done a different way. Certain reporting is not done. So, it is a process which can be used either for cataclysmic things or for trivial things. And it will be part of our arsenal. What happens with PDP 3.0 and other things, I'm not even going to talk about in this forum right now. Joanna.

JOANNA KULESZ: First of all, that is a humongous task. So, kudos guys, for putting up with this. It's amazing and it's challenging, and I hope the ATLAS III exercise will somehow fuel --
ALAN GREENBERG: And frustrating.

JOANNA KULESZA: I would imagine it might. So, first of all, thank you for taking this on. Still being impressed by the conversation we had in a previous session, and I'm not prophesying anything but just asking the question, what happens if we can't do it? What happens if we can't have a uniform system? Is this being considered? Or, to flip that question around, would it be easier if we somehow fragmented the network to have GDPR and the EU and different frameworks outside? And if it's an abstract question, just say, "That's silly, Joanna. Let's just move on." Thank you.

ALAN GREENBERG: There is 175 different privacy legislation actions either in place or being developed. We're not going to go back to no privacy. The world has changed. You like it, you don't like it, doesn't matter. It's changed. So, we are working to GDPR because it's a well known and widely used framework. But it's not the only one. So that's a reality. What happens if we can't come up with any level of standardized access? We're doing it today. You go to the registrar or registry, they may or may not answer you. They each have separate rules and separate forums. The world will keep on running. Maybe well, maybe not well.
Chances are we will have a centralized entry into it. We will probably have some level of accreditation, because that will help the registrar, registry when they're making their own decisions, if they know who you are, and are you someone who is trustworthy and you've promised on a stack of some things that you're going to be a good boy or girl.

So, we'll likely have some level of organization, even if we don't have centralized decision processes. The world will keep on going whether it works well or not, whether malware will increase or decrease, whether whatever -- intellectual property. People will tear all their hair out because they can't take action. The world will keep on going one way or another. Maybe well, maybe not.

HADIA EL MINIAWI: Just quickly, I don't see us ending up with nothing. Definitely, we'll end up with something, in relation to uniformity or standardizing the system. But how much of that, that's what we're talking about.

BARTLETT MORGAN: Obviously, first of all, congrats on all the really hard work you guys have been doing. It's just a lot of work and I think it needs to be acknowledged. But just quickly, a lot of the conversation I heard earlier had to do with the whole uncertainty around ICANN's liability, joint control and that kind of a thing. So I just want to quickly jump in because I remember about two months ago, the ECJ delivered this decision called Fashion ID. So I don't know if you guys within the
EPDP have just had a look at that decision, because it did go some way towards clarifying the whole notion of how much your liability will be as a joint controller, that kind of thing. So I just wanted to throw that in there.

ALAN GREENBERG: We haven't determined who is a joint controller, or whether we're independent controllers or what. There is some claim that we could say that for most of the data collected, ICANn is a sole controller. We could make that claim. Not everyone agrees. Of course, ultimately, whatever we claim will depend on whether European data commissioners actually agree with us.

BARTLETT MORGAN: Which is a part of this whole, almost chicken and egg type situation. Because as you've mentioned earlier, it's really 157 different laws. And those different laws will determine whether or not the whole concept of a joint controller exists, versus an independent controller and that kind of thing. So it really is a tough task.

ALAN GREENBERG: Nevermind the different laws, it's different people interpreting the same laws, in many a case, and they may have different versions of it. The Data Protection Board is an attempt to bring some unification and consistency among the European countries. But it's not guaranteed at this point.
GREG AARON: Tijani.

TIJANI BEN JEMAA: Thank you very much. I don't see how ICANN will live with something without any standardized or unified model, because at the end, ICANN has certain liabilities and it will be affected by what will happen if there is a problem with a registry or registrar. So, everyone having their own rules, their own ways to do with the access, I don't see how ICANN will live with that.

ALAN GREENBERG: Ultimately, there will always be complex cases which are value judgments, and the registrar is likely to be the one to make that value judgment in some cases. To what extent they act in similar ways across the whole body of registrars, who knows?

GREG AARON: Dev.

DEV ANAND TEELUCKSINGH: Kudos again, as that is echoed, about the model work that has been done on this. I guess my question is, I'm trying to understand this, what about the IP addresses side of things? The WHOIS of a IP addresses, there is a system where who has access to an IP address
and so forth, is the EPDP looking at that aspect of it, or is that handled or solved already? What happening on that aspect of it?

ALAN GREENBERG: We are not looking at that. We are looking at the domain name WHOIS for gTLDs only. Different bodies have taken different positions. There are European ccTLDs who publish personal information. The RARs publish in general have decided that there is legitimate reason for publishing personal information in some of the IP address WHOIS and the other numbers they -- different entities have made different decisions. Each of them subject to the laws of their own jurisdiction, which will be allowed to stand or not. We're certainly not looking at those. People have raised those as examples why we could do certain things. In general, people say we don't care what they do.

GREG AARON: Thank you for all the questions. Alan and Hadia, any closing remarks?

TIJANI BEN JEMAA: May I add one word? ccTLDs are out of this discussion because ICANN doesn't have any contract with them. So it is not an ICANN issue.

ALAN GREENBERG: Thank you for helping us fill up the time and ending 30 seconds early.
MAUREEN HILYARD: I would like to also add the thanks from the At-Large community, to you, for the amount of work that you guys have actually put into this. It's been absolutely amazing. Thank you very much.

Our next session, of course, is a working session over lunch. And I'm not quite sure, does it look like it's nearly ready?

GISELLA GRUBER: Yes, so lunch for the At-Large leaders and ICANN66 funded travelers, as well as any ATLAS III participants we have here. Please, you're welcome to help yourself to lunch at the back. And if there is an opportunity, we'll open it up to anyone else who is around. Thank you.

MAUREEN HILYARD: So if you'd like to go and get your lunch, come back, get organized. And then we will have the ATRT3 and the NomCom during the presentation, during your lunch break. Thank you.

[END OF TRANSCRIPTION]