ICANN
Transcription
Next-Gen RDS PDP Working group call
Tuesday, 14 February 2017 at 17:00 UTC

Note: Although the transcription is largely accurate, in some cases it is incomplete or inaccurate due to inaudible passages or transcription errors. It is posted as an aid to understanding the proceedings at the meeting, but should not be treated as an authoritative record. The audio is also available at:
MP3: https://audio.icann.org/gnso/gnso-nextgen-rds-pdp-14feb17-en.mp3
Adobe Connect Recording: https://participate.icann.org/p8cl9zjxi06/

Attendance is located on wiki page: https://community.icann.org/x/dpDRAw

The recordings and transcriptions of the calls are posted on the GNSO Master Calendar page http://gnso.icann.org/en/group-activities/calendar

Coordinator: The recordings have started.

Terri Agnew: Thank you. Good morning, good afternoon and good evening. Welcome to the Next Generation gTLD Registration Directory Services to Replace Whois call on Tuesday, 14 February 2017.

In the interest of time there will be no roll call as we have quite a few participants. Attendance will be taken...

((Crosstalk))

Terri Agnew: ...via the Adobe Connect room so if you are only on the audio bridge could you please let yourselves be known now? And again, Daniel, we have you noted. Hearing no further...

((Crosstalk))

Chuck Gomes: ...Daniel?

Daniel Nanghaka: Daniel is here.

Chuck Gomes: Got you, Daniel.

Terri Agnew: Thank you. Hearing no further names, I would like to remind all to please state your name before speaking for transcription purposes and to please keep your phones and microphones on mute when not speaking to avoid any background noise. With this I'll turn it back over to you, Chuck. Please begin.

Chuck Gomes: Thanks, Terri. And welcome everyone to our call today. I think it will be an interesting one and hopefully a productive one too. Does anyone have an update to their statement of interest? Okay, not seeing anyone or hearing anyone let's go on to the main part of our agenda starting with Agenda Item 2.

And in preface to that, I want to make a couple comments. First of all, I've appreciated the live active discussion that's been going on on the list; I especially appreciate some new people that we haven't seen saying much joining in. You're very welcome and some good points have been made. And so it's good that more people are getting active. And hopefully we will see that as a continuing thing as we are really getting into the nitty-gritty of our work.

Now I want to remind everyone that, you know, we can only cover so much at a time and be effective. Right now we are focusing on data protection and privacy. That doesn't mean that we are giving priority just to that area to the exclusion of other areas like rights protection and law enforcement and so forth so please be patient with us.

What we're doing shouldn't be looked at as just focusing on one area at the exclusion of others but look at it as a task that we're doing right now to improve all of our understanding of this particular area. It's very important that we have as good an understanding as a group about data protection and

privacy regulations in different jurisdictions just like it will be that we understand the needs of rights holders, of law enforcement and so forth.

So please don't assume that we've made any final decisions on what we're going to do. A lot of you have been talking about things that are a little ahead of the game and that's okay. Most of you recognize that we are going to get to those issues as we move forward. Right now we're focusing on thin data and we will get beyond thin data hopefully in the next few weeks or month or so.

So bear with us. And understand that what we're doing right now is - and right up into Copenhagen and shortly thereafter we want to get as good a understanding of data protection requirements as we can because that will help us come to solutions that address those requirements while at the same time addressing other needs that sometimes come in conflict, often come in conflict with some of these requirements. So bear with us.

And certainly use opportunities like today to bring up your points as related to our particular topics. And especially ask questions that help us all get more clarity on the challenges in front of us. So I'll stop with that and let's go ahead and bring up the slides for today's meeting.

And I'm going to - we're going to start off with a slide from the presentation that Stephanie Perrin prepared for last week but she didn't give it because Peter gave some slides. So you'll notice this is a - we pulled one slide out of Stephanie's presentation that she had prepared that I thought was a pretty good transition from our discussion last week when Peter gave a presentation and Peter and Stephanie discussed with the rest of you on the call some of the things with regard to privacy - data protection in particular.

Notice the two bullets here. One of the things that we're focusing on right now is the purpose limitation in particular in European data protection law, but I think it applies in some other jurisdictions as well. And the first bullet you can

see it there, a broad interpretation of the purpose of collection, use and disclosure allows some subsequent reuse for different reasons.

Now that's not a - that's just a comment from Stephanie in the sense that - in other words, if you interpret data protection requirements very broadly, you would allow it to - you'd be allowed to collect, use and disclose, you know, a broader set of data. Obviously a narrow interpretation would do just the opposite.

We haven't decided yet but will have to decide exactly what data elements would be collected, what data elements would be used and disclosed and we're mainly focusing on collection right now.

The second bullet, purpose limitation, and Peter and Stephanie talked about this last week, purpose limitation is the first premise of data protection analysis - and the purpose must be narrow and proportionate. How narrow? We're going to have to decide, okay? And some of you are legitimately concerned about too narrow a definition there.

Others are concerned about too broad a definition. So the purpose of this slide is just to kind of bring us back or transition from what we talked about last week and as hopefully all of you know, we didn't finish last week on this area so we're continuing that. And what the leadership team decided to do was to go over some examples from Peter and to have Q&A on those examples after each one and then we'll move on from there. But let's go ahead and go to Slide 2.

And I'll turn it over to Peter.

Peter Kimpian: All right, thank you. Thank you very much. I hope you are not too much bored about my presentations. This time I would like to be - to have it more pragmatic way, I mean, in giving you more life examples and from outside of

ICANN environment that we have come across or some court cases was about especially in Europe.

But as always, I try to have - and to prepare myself for this presentation as - in looking at a global picture as I keep repeating, privacy is a human right, which is globally recognized. We have different legislation in this. We have for the moment one international legal instrument for this. But we have different - we have different privacy frameworks or international instruments, I would say, which are not legally binding, however, it can guide us through well the implementation.

For today's presentation, I would like to speak about the - as Chuck said, the very fundamental principle of purpose limitation or purpose specification. And for this, I have chosen the language - and it's only because of the language, let's put it, like this and because of course I'm representing Council of Europe and the Convention 108 is the - to date is the only international legal instrument on data protection and privacy, which is widely recognized in the world.

However, as I said, it's not the only framework. The only binding one, but of course not the exclusive one. However, it has very - and more importantly, the modern version of the Convention 108 has a very self explaining language about purpose limitations. So - and the main principle. So I put this on the slides. But before this, to - as a proof of what I have just said, I will again, start referring back to the APAC privacy framework which under the third chapter we have the principle of collection limitations.

And in this text it says that the personal information should be limited - the collection of the personal information should be limited to information that is relevant to the purpose of collection and any such information should be obtained by lawful and fair means and they're appropriate with notice to or consent of the individual concerned.

So here you can already see the identical languages that those two texts uses. But here I will jump to the modernized convention text which says that the data processing shall be proportionate in relation to the legitimate purpose pursued. And I will stop here a little bit because this is the core essence I would say, of the purpose limitation principle. So when we are processing data (unintelligible) the proportionate to the legitimate aim or the legitimate purpose pursued.

And what is the legitimate purpose that we have to - we have to define it in advance. And well I - basically I don't want to repeat but what I have said through the - during the last week's presentation you will find a set of principles on the - on the slides. And I have underlined some of the - the most important one as the lawful processing and the second - under the second point, the free (unintelligible) concern and so on and so forth.

But for the - to be very pragmatic I would say that to process the data you have to - you have to define your purpose for what you are processing it and this has to be proportionate, I mean, your action and the data processing has to be proportionate to this purpose pursued.

So with this, I will go to the practical example. Of course we can go back to the principles, but I think we have already said a lot of things about those and the practical implementation of those principles. And now I will like to turn to the examples for purpose specification.

And these are for the, yes, for the - for all of them are real life examples which are coming outside of the ICANN environment. But these are not innocent examples because it can be, in my sense, related or - or we can relate them to ICANN - ICANN's work and ICANN activities.

So to start with the first one, I would like to - this is a very famous one, I mean, in data protection community when the retail company and consumers health conditions. So it happened somewhere sometimes, I don't want to be

very specific in that because it doesn't matter, but it happens actually in Europe.

So it was one company who processed one consumer personal data under a contract of loyalty card. So this consumer had a loyalty card and when he - about articles in this - in the retail - or in the store - he used - or actually she used the card. And the company used the data for - for a better service to assess better what kind of articles this consumer is looking for.

And this company also used a kind of analytics in its processing methods. So with using this big data analytics they found out that their consumer is pregnant. So they called up the given number to - for telemarketing purposes and to have a direct offer of diapers, which of course was offered to her in a - for a very competitive price.

But unfortunately, it was not her who pick up the phone but her father who was not at all aware about his daughter's situation and her daughter's pregnancy. And it was during the call the retail company who revealed this and the whole conversation went very bad.

So you can see that to be pregnant, it's not a marketable thing anymore or it's not - maybe it's related to personal data. And you can find out because there are a lot of tools, a lot of possibilities now to find out and find out a lot about consumers' health or other type of situation.

But this retail company cannot have or doesn't have a purpose for have condition, I mean, for - the data was not processed by this retail company for medical reason because as retail company cannot process or of course I'm exaggerating and I'm simply oversimplifying but let's put it like this bluntly that a commercial company will not be able to process data for healthcare reasons or under - or they can process under very strict conditions.

With this, let's move to the second example, the personal data collected by drones. So drones are very fun things. It was like they were just hitting the sales in most of Europe in countries. It's really - and not only in European countries but I think across the world, it's really on rise. However, there are also - we found out that there are also some privacy and data protection consideration when you are using drones.

And actually it happened to me when it was - I was in vacation with my family and suddenly a - on the beach - and suddenly a drone appeared above me and not only above me but above 100 of person. And we know - and it was obvious that it was making recordings.

So that again an example, where you have privacy concerns that needs to be taken into account in advance and you have to be very specific with your purpose limitation or purpose of processing your - purpose of processing personal data and the person and the data subjects of which you want to process the personal data.

Because the drones - and I explicitly use this example because with drones you can very, very easily process personal data of person who are not aware about the data processing and maybe you are also not - I mean, you don't want to - that kind of processing. But once it occurs, it breaches most of the privacy legislation and like - which is like this.

We have a very interesting case at the court - because what's happening is if I'm alone and also I saw this kind of videos as well on the Net and they're splendid and (unintelligible) but when you're - oh something is happening.

Chuck Gomes: Everyone, please make sure your phone is on mute except for Peter.

((Crosstalk))

Peter Kimpian: Hello?

((Crosstalk))

Terri Agnew: And this is Terri. We're trying to isolate the line.

Chuck Gomes: Thank you, Terri.

Peter Kimpian: All right. Okay, maybe I was saying something stupid. All right, so this video when the people - when a couple is on the beach and they are filming - they are filming each other that's perfectly fine, no - anybody else - or nobody else is on the beach. And they can use new technology, they can have fun of it. And that's fine. But if we are on the street and they are doing the same thing, I mean, inevitably they will start recording other people because you are on the street.

And this is why a court in a court case the European Court of Justice said that- it was a journalist case. The journalist went outside in the street and started filming - it was not with a drone but started filming in a public space. And it was contested. And in the contrary argument the journalist said that it's for his own purpose and he will never go on public with this.

But the court said that on the street you have to have the expectations that you will not be filmed and you will not be - your image will not be captured without your notification, without being informed, without a specific purpose that if you allow - if you are processing personal data and it is in public space, you have to follow data protection regulations even if it's for your own use. This was quite revolutionary; it was very contested later on. But still, it's a good example to show you how the purpose specification is important in a real life situation.

Let's move on to the purpose and the public authorities. And purpose specification for public authorities because public authorities of course processing personal data, and for them also it is very, very relevant and of

course mandatory in most of the jurisdiction to have a purpose specification, very common and to understand why it is important.

Law enforcement and - we are saying in general terms, law enforcement, the police, or yes, or national security agencies, but if you are looking at the legislation they have construct or they have - gave birth to those bodies or to those organizations it was a for a reason. And the data processing has to be in relation with those reasons why it was - they was constructed.

So for instance, an immigration authority, a body who is responsible for immigration was not created for fight against crime; it was created because of immigration purposes. So it's a very common - very common mistake, I would say it like this. And the very common concern from people that their immigration data will be used for law enforcement purposes as well, which is not possible according to privacy legislation because the purpose will be not the same.

There are some conditions under which certain data, in certain cases or some - in some investigation it can be used, but for this you have, again, a case by case purpose specification.

And I will finish by the digital island and the (tele two) cases because I think it's relevant - it's not a Council of Europe and the Court of Human Rights cases, it's a court of the European Union who made - who pronounced the judgment on these cases. But it's very relevant I think in ICANN context as well.

We had, in Europe - in the European Union - a directive which foreseen the - which has foreseen the retention of electronic communication data but only, not the content, hopefully, but the - how you could say - the meta data and the communication data.

And this case was contested before the court and the court said that this practice is infringing right to privacy and to the protection of personal data. It said that it has, and I spoke already about this during last week's call, it represent an interference with the fundamental rights. And the interference is - if it's there it has to be balanced. And the courts found out that the balance was not right because there was no subjective criteria under which this data was retained.

I mean, it was a blanket format for the retention of any of the data. It was not specification, again, purpose specification. So for which purpose? For - whom data and for how many period and so on and so forth.

So this judgment of course and the court verdict is much complicated than this, but I would like to point this out that this purpose specification questions comes back and back again and again in every, every big cases before the court. And they are - they are looked at it in a very total way. And the data controller under European regulations explicitly and starting from 2018 more explicitly will have very stringent obligation on - about the fulfillment of this principle so how to - how to apply the purpose specification and how to be as precise as possible about the purposes of my - of my data processing.

So basically, that was it. I have another slide which only a slide for reference for you to - a set of examples which was produced in an Article 29 working group's document, you will see now on the slide and you have the link from the - I think 51 page onwards, you have too an access and they have plenty of examples about purpose specification and about the (unintelligible) assessment, how you - as data controller how you should pursue this.

So I think that's it. I covered all this - the examples I had in mind. Of course it was not very much ICANN specific. But I chose them as I said, not innocently. And we had some preliminary discussion about the ccTLD, which now I will not start to assess and their practice about purpose specification. But we found out that what is more important is to first specify the Whois

purposes because if we specify the Whois purposes which will be in relation, of course, with the ICANN purposes, it has to be in relation to the ICANN purposes, then we can go further on specific application of gTLDs - I mean, on their specific implication in the gTLDs or the ccTLDs contracts in terms of reference.

So I stop here and thank you for the opportunity again. And I'd be happy to answer the questions if you have.

Chuck Gomes: Thank you very much, Peter. Appreciate this. I'm going to open it up to questions for the whole working group just shortly. And I'm going to ask a few to get it started. If we could go up to Peter's second slide please? By the way, this is Chuck speaking.

Okay so the first question I have for you, Peter, is tell us a little bit about this modernized Convention 108 Article 5. Is that a law that applies to people in Europe? Is it a law that - how does that apply to us whether we're in Europe or not? Can you comment on that a little bit?

Peter Kimpian: Yes, I mean, the - there is again the beeping.

Chuck Gomes: Sorry about that. Terri's acting on it to get - mute that line. Again, please keep your phones on mute.

((Crosstalk))

Peter Kimpian: Okay so as I said, there are a lot of - so there are multiple legislations throughout the world. One wonderful gentleman (unintelligible), has, yes 110 legislation on data protection in its study always available and can be consulted. But I used those references and I used this text because this is what I know the best.

And because this Convention 108 is, as I said, the only international treaty - international convention on privacy and human rights. Of course, it would be wonderful if we could have one under the UN and all of the states could sign to it for once, I mean, in a simplified procedure. But there are not too many chances, to be very honest, in my lifetime at least, to arrive at this.

But being said that, the modernized - the Convention 108 is an open convention. And in assessing the advantages, first states can get out of it, first states started to join outside of Europe Convention 108. For now we have three but we have in - who has joined Convention 108 outside of Europe, we have 47 member states in Europe who are members and party to this convention. And for them, it's a binding legal text.

And three out of Europe has already joined. And they are - and for them they have - it has a binding effect. And we are in negotiation with more and more and rising number of countries which, for economic reasons, I be very open on this, and for other reasons, they are considering of joining - joining the Convention 108.

Economic reasons because Convention 108 is based on the free - the promotion of the free flow of information so - and the free flow of data. So basically it - among their member states it - it enables the free flow of data. So basically and to put it very, very - in a simple language, if you join you can send and receive data without taking care about national legislation, let's put it like this.

For instance, in Germany, if I'm not mistaken, the national law said that all states that has joined Convention 108 are qualified as having an adequate level of data protection and so on and so forth, there has a lot of reasons, political ones, (unintelligible) political ones, and the economic as well. But this is why I'm making all this reference and because I'm working for Council of Europe and this is a Council of Europe instrument. But it is much, much and

very widely supported by the European Union, European Commission as well.

So and it has a really global advocacy and we are really in the phase of looking for more and more countries to convince them and not only convince them but to have them to join this convention which can facilitate a lot of things in our very difficult world with sometimes fragmented data protection and privacy legislation.

Chuck Gomes: Thank you, Peter. We have a couple hands raised. This is Chuck. Theo, are you going to follow up on the Convention 108?

Theo Geurts: No, Chuck. This is Theo for the record. I was actually...

((Crosstalk))

Chuck Gomes: Hold on a second. If you're not going to follow up on Convention 108 let me hold a little bit. Alex, are you going to talk about Convention 108, a question or a comment? Okay...

Alex Deacon: No, something else.

Chuck Gomes: Oh okay. So hold on. I'm going to call on you, I just wanted to make - I definitely wanted to have you jump in if you were going to talk about this. I think Peter answered my question. There are jurisdictions, certainly it sounds like most European jurisdictions, have joined this convention so these things would apply. That doesn't mean that others can't do that.

So all right, Theo, let's go ahead and go to your question or comment.

Theo Geurts: Okay, thanks, Chuck. And thank you, Peter, for the explanation there and the examples there. And what I'm hearing is a sort of recurring theme that the collection of data has to have a legitimate purpose. What I'm also hearing is

that the companies that are processing the data have to make sure there's an adequate level of data protection.

And when I'm looking at sort of the ICANN field scope, field maybe the best word here, my English is not my primary language, but anyways, what we are doing is we are sending the data to these registries which could be - could have a legitimate purpose, but then the data gets completely displayed in a public Whois. I don't see how we can have any data protection safeguards there when we just open it in public.

And that sort of follows through the examples that I've been hearing. I've been hearing that in certain examples that certain companies sort of been -- they actually had issues with a European law there and apparently there was some kind of wording there that it was not legitimate.

And I'm actually wondering if we are going to proceed with this endeavor, how are we going to make sure that once we are at a stage where we are finalizing stage of the RDS that we are complying with European law and all these other countries who have some kind of data protection or data privacy law? Because it feels like we're going to open a can of worms there which is pretty big there. Thank you.

Chuck Gomes: Thank you, Theo. And you're asking great questions. In fact one of the questions you're asking is really under Item 3 on our agenda as to whether or not for thin data we are currently in compliance with our Whois with data protection requirements, so we're going to get to that, okay, we're going to talk about that. And then of course how we would implement all this is down the road a ways. We first of all have to come up with the requirements and right now we're looking at possible - we're kind of heading into possible requirements with regard to data protection. So we're going to get there. Your questions are great.

Let me go to Alex. By the way this is Chuck speaking.

Alex Deacon: Thanks Chuck. It's Alex. I had a quick question on the first slide, the two bullets from Stephanie. I was just curious, are those a reference from, you know, a long regulation or something or are they just statements from Stephanie? I'm just curious to know kind of the origin of these two bullets.

Chuck Gomes: Thanks Alex. This is Chuck. Now Stephanie is the also she may not be able to speak so I'm going to propose an answer. Certainly Stephanie, if you think you can speak just raise your hand but I won't put you on the spot because I know you're having problems with your voice and that's fully understood.

These are statements from Stephanie as I understand it. Now her statements are coming from some of the documents that we have those resources like for example the Article 29, the Working Party 203 opinion that she summarized, and also you can see some of this comes from -- is very closely related to what Peter presented today and presented last week. So don't worry too much about whether these are, you know, statements of fact or Stephanie's opinion.

We put this slide up there mainly to kind of transition from what was talked about last week and this whole idea of purpose and purpose limitation or broad purpose or whatever. So Stephanie has raised her hand, let's give her a shot. Go ahead Stephanie. Your voice sounds really weak; we can't hear you. Looks like you're off mute. Okay Stephanie, we can't hear you. Let's go ahead - Alex, I hope -- I don't think my answer was too far off. But don't worry too much about whether those are opinions or factual statements.

I mean, they obviously -- the first one is obviously just a statement. I think it's accurate, you know, if you interpret the need for a statement of purpose very broadly you get different results and if you can - then if you interpret it narrowly. And we're going to have to decide how narrow or how broad we will interpret these things.

And in some cases in some jurisdictions if you look back at Stephanie's summary of Article 29, you know, it talks about very - that the statement of purpose has to be very explicit. But it also has some flexibility built into it. When I read that, I particularly look at that again this time.

And let me read that purpose specification that's in Stephanie's summary of that document that we address the long time ago. It says, "Data collected only for specific explicit and legitimate purposes. Purpose specification determines the data to be collected, retention periods and all other aspects of how data is processed must be determined prior to or not later than collection. Each separate purpose should be specified in enough detail to be able to assess whether collection of personal data complies with law and what safeguards are necessary."

Bypass I went on in that document I also noticed, and I'm kind of addressing - there's a section there that's on exceptions under Article 13, and there are exceptions for national security, for defense, for public security, I won't read them all. But one of the last one is the protection of the data subject or of the rights and freedoms of others.

So please comment as we're looking at this I think it's clear that we need to -- we're going to need to focus on the purpose of an RDS, and I have some other questions in that regard following up on Peter's, but let me first of all go to Mark.

Marc Anderson: Thank you, Chuck. This is Marc Anderson for the record. And I first wanted to thank Peter. You know, I found your presentation, you know, this week and last week, you know, very useful or relevant, informative. You know, I've been participating in, you know, the policy process for a number of years now. And, you know, having, you know, being able to benefit from your expertise and participation is a real luxury so thank you for your time and your participation here.

But I also, you know, wanted to, you know, maybe echo a little bit of what, you know, Chuck was saying about the purpose, you know. You know, a couple months back we spent some time deliberating on the purpose of RDS. And I think we struggled a little bit and people started to get frustrated and we sort of abandoned that effort. But, you know, some of our more recent discussions, and certainly from what Peter has spoken to us about, you know, I think it's, you know, very important that we take another crack at defining what the purpose of RDS is.

You know, it seems like that's going to be an important step for us to move forward with a common understanding because I'm sure there are many different views within this group on what the purpose of RDS is with all the different views out there it makes it that much harder for us to move forward coming to a single solution.

You know, I may end on asking Peter if, you know, if I could put him on the spot if he had some advice. And, you know, I note, you know, Peter in your slides you provided some examples of purpose statements, but if you maybe had some advice or suggestions that would help us in our deliberations in moving towards defining the purpose of RDS. Thank you.

Chuck Gomes: Thanks, Marc. This is Chuck. Peter, go ahead.

Peter Kimpian: Yes, thank you. Thank you very much. First, I just wanted to come back very shortly in Chuck's answer or Chuck's question or comment and it will answer - it will answer others' intervention as well. So why I'm here and why I'm speaking to you about all this and how this relates to ICANN. First of all, maybe you are aware or maybe not, but at the Council of Europe 50 governments - 50 states in Europe at the Council of Ministers published or agreed on a declaration which is setting the organization position or organization strategy towards ICANN.

And they felt that human rights and the rule of law and the implementation of this very broad principles have to be - have to be followed - the implementation of those principles have to be followed and if needed assisted by the Council of Europe. So basically this is why I'm here because we felt that the privacy - the right to privacy and right to data protection are one of the human rights which is the most affected by - not the only one but the most affected by ICANN policies. And this PDP RDS is one of the best example for this I think.

Why I'm referring to Convention 108 all the time because as I said, it encompasses all the internationally recognized data protection principles. It doesn't have anything which is not shared or not followed by any of the countries having 110 countries having data protection and privacy legislation. And it is not only recognized by us because I'm saying you this, but you will hear the United Nations special rapporteur on privacy will saying the same thing. And others privacy experts will you the same thing.

This is why I'm using also APAC privacy framework as a reference and to show you the parallelism of it is because basically this is not meant for Europe APAC, this is Asian Pacific, so this is basically to, again, put it very simplistically, it's American law and American way of dealing with privacy.

But it's at the same thing, and I have been working very, very hard with colleagues on privacy, that was involved in this work. And we have found all the translations we can have about EU and US legislation because ICANN is - we hear very often that ICANN is a California law-based company so they have to follow this legislation.

But all in all, and I will finish on this, if we take Convention 108 and if we read it and we - and if we follow the provisions and principles we can - we have a common minimum (unintelligible) in our hands. So this is why we think it's useful and it's useful in a global context.

And to give you a very concrete example how to - and to respond to the question, which has been put, I think we have to read first the bylaws of the ICANN and after we have to give it a try to suggest something which is - which is purpose specification. And for this we can have of course what we have been doing or, yes, we have been doing since months, to find the possible purposes data can be processed under ICANN remit. But after we have to apply what we call in Europe the balance test.

And for this there is a methodology and I can help you. I'm here for this to help you out of this if once we reach there, but we have to take one by one and to apply the test how to - whether if it can be designed or it can be taken as a legitimate purpose for ICANN mission or ICANN activities and publicity of data is one of them. We have to use the balance for this whether we are defending or not others interests by hurting data subject rights.

So that's a whole legal exercise we have to carry on, but we are here for helping you out with this.

Chuck Gomes: Thank you, Peter. This is Chuck again. And going back to Marc. Marc, yes, I think you're right, we're going to have to work on a statement of purpose. A lot of people are doing that in the chat. There's some good ideas in there and we're going to have to - that's going to be a challenge. We have on the agenda today to look at an example of a purpose statement, and of course there are lots others. And I think Peter provided a link where some guidelines in terms of developing purpose statements. We probably will look at that in more depth.

I understand that Stephanie now has audio so let me give Stephanie a chance to talk if her voice will let her.

Stephanie Perrin: Thanks very much, Chuck. Both bullets that I think it was Alex was asking about, I'm just getting rid of my echo here, sorry, actually were my summary for the purposes of the presentation. But I think it's based on having a broad

look at how we have drafted data protection law in the various jurisdictions. And if you're interested in reading on this I would recommend (Lee Bygrave) who has been advising on the transition is also a data protection scholar and he has a book called Data Protection Law that looks at how the various concepts and data protection have been implemented in practice.

And I also looked at Greenleaf and what Greenleaf had to say about this. The purpose limitation has been there forever. It was in the OECD guidelines. It was in the original Council of Europe Convention 108. It is broadly accepted to be the fundamental step in figuring out how you manage the rights that an organization has to process data. Thanks.

Chuck Gomes: Thank you very much, Stephanie. It's Chuck again. I have another question with regard to purpose. And then I'm probably going to propose a conclusion to see if we can agree on it on this call and then follow up in a poll. But not so much recently but going back a ways there was talk about primary purposes and secondary purposes.

Now I confess that I did not - or do not fully appreciate the difference between primary purposes and secondary purposes especially with regard to some of the data protection things that Peter and Stephanie have been sharing with us. Are secondary purposes exceptions? Or what's the difference between a primary purpose and a secondary purpose with regard to this need to limit purpose and to explicitly state purpose? Let me put that to Peter first and then if Stephanie wants to respond and then if anybody else wants to respond.

Peter Kimpian: Yes, thank you. Thank you very much. I think my answer is very simple and clear. You don't have to bother about secondary purposes. It is not you that - I mean, not the controller who has to bother about secondary purposes but the data controller of the - of the further data processing. So to again to put it very - in a simple example, for example, the immigration data.

The immigration authorities doesn't have to bother about whether this data will be used or will be good for law enforcement purposes for fight against drugs, for instance. They have to be sure that this data is collected, is collected under the conditions and under the circumstances it has been prescribed by law or by other means. It is accurate. It is processed fairly. It is obtained in a lawful way.

And so (unintelligible) and you don't have to bother about the secondary purposes, whether if it will be used for statistical purposes 30 years later or it will be used for I don't know, okay, let's take a police example, the drug trafficking, it is for the police who will pursue the drug trafficking case who will account to the immigration authority to prove that, hey, I'm here a legitimate purpose, please give me your data. And that's it.

The immigration the first grade or first level data control doesn't have to bother about the second, third and further use of its data. Period for me.

Chuck Gomes: So, Peter. This is Chuck again. Let me pursue this a little bit further. So in our case, in the ICANN world, within RDS, I think most of us would - probably all of us would agree that a purpose of an RDS is to facilitate operational purposes for domain names. Now - and of course as well know it all started - Whois started to - for those technical reasons if there were problems in terms of resolution and so forth so that people could be contacted.

Now, let's add in now trademark protection. How do we address that in our purpose statement? Do we have a general statement of rights protection - that part of our purpose is to provide means to protect people's rights with regard to domain names? Let's bring it home to where we live in the ICANN world. Can you comment on that?

Peter Kimpian: Yes, of course. And I have very a simple answer to those questions as well, I think. But as you know, I'm - I'm a more - I have a more cautious approach and don't want to jump into this already. I think we have to specify what those

purposes means in real life. I mean, what - the purpose you refer to the mention and stuff, the domain name system, what does it entail? What are the actions, the actual actions you need to do to secure or to pursue this? And you - after this you have to render the data processing to those activities.

And for instance, there are secondary or third purposes or use of this data. But you have to decide what will be your, I mean, ICANN have to decide what will be the first level whether it will be - it will have the anxiousness about the trademark regulation or the implementation of the trademark regulation or law enforcement or, you know, other issues.

But for this, as I tried to point it out that you have also to take account and you also will have to balance one more thing that if you say that this is my first level of purposes, this is why I am processing personal data, that you have to bear in mind that you are accountable also for these purposes, that you will have to be - you will have to show all the - and to stand for all the requirements data processing needs according to privacy principles that you have to process it fairly, adequately in an up to date. You have to listen to the claims, you have to change data if it's necessary, you have to replace it, you have to keep it - and so on and so forth. Do you want this?

And of course it is very complicated because we are now in a - in an international or let's say globalized context. ICANN is not a - is not a data controller under one jurisdiction, I would say like this because it's pursuing its activities worldwide. So in a country, in a national legislation that would be so much easier it would have then some law which would prescribe it and it would be the parliament who will vote this legislation and will agree on that and it will give the necessary legitimacy for this legislation because at parliament we avoid it and it will be promulgated and so on and forth.

But for ICANN it has to define itself whether - what would be the first level or first grade purposes for which it will process personal data and decide it. I will

- and if we draw a line that here are our purposes before that, I think we should forget about all the rest.

Chuck Gomes: So, Peter, this is Chuck. Are you saying that our purpose statement for an RDS needs to be specific enough to cover not only what we might call a primary purpose but any lower level purposes?

Peter Kimpian: Well if we want to be on the safe side I would say yes.

Chuck Gomes: Okay, thank you. Stephanie, go ahead.

Stephanie Perrin: Thanks very much, Chuck. Stephanie Perrin for the record. I think this whole issue of primary, secondary, tertiary purposes, there are differences in the different data protection laws around the world so we express it differently. Certainly in Canada with the first privacy act, and I believe you had the same problems in the United States with the privacy act down there, one of the expressions that crept in was consistent use because we use the expression agencies can gather information for the pursuit of - let's take the education authority for the pursuit of providing education or for a use consistent with that purpose.

Well the problem because that just about anything became a consistent use. So successive generations of law drafters tried to refine this down a bit. And you can do it either in the purpose clause or you can find other clauses in your legislation where you define it down. It's done differently in our provincial legislation. So you have to look at the laws in their totality to figure out how this is grappled with.

If I could give you just one example that will show you why we really have to deal with that problem, I call in the 90s when we were doing some work on training manuals for the new law that was coming in and the new standard actually before the law, we looked at a daycare in the province of Quebec that already had data protection law. And they were - and this may appeal

may more to the ladies in this group than to the men, I don't know how many of you have young kids.

But who wants to hand over to a daycare all the details of your pregnancy, all the details of the birth whether it was a forceps or not, whether there was a cord around the child's neck? You do have to ask yourself, okay why does a daycare need this information? Well, it matched their purpose, you know, gathering health data to ensure the happiness of the child at the daycare. I mean, you have to buckle the purpose limitation clause down as tightly and specifically as you can.

Now in the case of ICANN, obviously the records show that at the time ICANN was formed there was a very real issue with what was happening with trademark and cybersquatting and all of the, you know, ills that largely the solutions have been found for some of these, although I'm not saying there isn't an ongoing problem. So the - the IPC and the - and WIPO certainly made recommendations to the Commerce Department that were listened to and Whois made the data available and the RAAs have continued to do so.

The question is whether that should be reevaluated in the case of risk nowadays and the various different technological ways we could achieve data disclosure. Doesn't have to be in the Whois. The other question is, is ICANN in its current state, set up to be the instrument through which trademark and copyright law are enforced? You know, possibly not. But that doesn't mean that you can't use data, but the question is how much data do you gather specifically for that purpose?

So I hope that helps. And I'm going to quit now...

((Crosstalk))

Chuck Gomes: Thank you, Stephanie. This is Chuck again. So I'm going to try to bring some closure, not very much, but some closure to what we've talked about today

and last week. First of all, I'm going to ask a question, Marc Anderson kind of hit on this in his comments. But are we in agreement as a working group that one of our - one of the tasks that we need to complete in the near term is to agree on a purpose statement for an RDS? And let me phrase it differently. I see a green checkmark. Is there anybody that disagrees with that conclusion?

And the conclusion again is, is that we as a working group need to agree on a purpose statement for the RDS. Is there any disagreement in that? And you're agreeing, is that right, Fabricio and Andrew? If anybody is disagreeing, put a red X in there, otherwise I'm going to assume that that's a conclusion we can test with a poll. Okay I'm not seeing any. And of course, Daniel, you can speak up if you disagree.

((Crosstalk))

Chuck Gomes: Sure, go ahead, Daniel.

Daniel Nanghaka: Previously I recall before the Helsinki meeting - it was after the Helsinki meeting when we went to start drafting the problem statement (unintelligible)...

Chuck Gomes: Daniel, you're breaking up quite a bit. I'm having trouble understanding you. Did someone else understand it better than I did? Please speak up if you did. Let me ask you - do you - are you in agreement that we need to develop a purpose statement for the RDS, Daniel? Could you answer that question yes or no? Or...

((Crosstalk))

Daniel Nanghaka: I make a statement I agree or not, I would like to find out about the previous problem statement that we came up after the Helsinki meeting. Does the

statement of Helsinki, is this still valid? If isn't valid then I agree that we should come up with a new problem statement.

Chuck Gomes: Okay so you're talking about a problem statement. Lisa, go ahead and respond.

Lisa Phifer: Chuck, I think Daniel is only on the telephone. There has been a fair number of comments in chat that we did have a draft purpose statement and that draft purpose statement is still in our working document. It's in Section 2.3. And it will be the next thing that we address when we get back to the charter question on purpose.

The problem statement has also been published and is still a problem statement for this working group to address. But I think, Daniel, what you meant to ask about what the purpose statement.

Daniel Nanghaka: Oh okay. Daniel for the record. Then I agree that we need to come up with one. Thank you.

Chuck Gomes: Thank you, Daniel. Appreciate that. Okay, so that conclusion that we need to agree on a purpose statement for an RDS is one we'll test in a poll this week. So - and certainly we want all of you to participate so we get more data but also obviously to give opportunity for those who are not on the call to participate.

The second thing, I want to jump very quickly, we don't have very much time because there's another item we need to take care of, I want to jump very quickly to Item 3 of the agenda, and there's a question there. And I'm suspecting we might already have the answer, and I'm going to ask you to respond, so please remove your green checkmarks. I don't think there were any Xs so for now if you haven't' done that.

Question 4.1 says, “For thin data,” and we’re only talking about thin data right now, “do existing gTLD registration directory services policies sufficiently address compliance with applicable data protection privacy and free speech laws about purpose? If not, what requirements might those laws place on RDS policies?”

I’m going to just focus on the first part of the question. It seems to me that we’ve come to a point where we recognize that the existing Whois does not address compliance with applicable data protection, privacy and free speech laws about purpose. We don’t really have a, I don’t think, an agreed-to purpose. We all have our own opinions what the purpose is. We’ve started work on that.

But am I correct in concluding that the answer to that question in 4.1, and I don’t know, can we bring that up there, Lisa or Marika, the - thank you, so look at that question at the top, okay? Can we agree that the answer is no? They don’t sufficiently address compliance with applicable data protection law even though data protection law varies by jurisdiction, we know that.

But certainly there’s some areas where it does not meet the protections if for no other reason that we don’t have a good purpose statement. Is there any disagreement with that? I see some green checkmarks. If you disagree with that statement, put a red X in there or in case of Daniel, just tell us you disagree.

((Crosstalk))

Chuck Gomes: So what did you say, Daniel?

Daniel Nanghaka: I agree with the statement.

Chuck Gomes: Thank you. Thank you. Okay so in other words, we - the answer is no to that first question. So that would be a second question to test in a poll. And again

we want everybody to participate in the poll whether you're on this call or not, but especially it gives an opportunity for those who are not on the call. Okay, so those are two conclusions that we're going to test in a poll this week. And you'll have a short turnaround so that we can keep moving.

But there's one other thing I want to cover before we close today and that is I have proposed to the leadership team, and I may have said something about it on the full list, I don't remember, that we form a small group. As everyone, I think, knows by now, and we talked about it last week, Peter talked about it, we're going to have a cross community session in Copenhagen with European Data Commissioners. Thanks, Peter and especially for his work and Stephanie's work for arranging for this and coordinating with the Data Protection Commissioners and arranging them to participate.

It's my view that we need to have some very good questions for those data commissioners, whether they're asked in that session or in our working group session on Wednesday afternoon with I think at least one of them can be there most of the time on our meeting on Wednesday afternoon there. It seems to me it would be very helpful if we had a group of volunteers, maybe one or two from each - one - not more than two, one's okay, from different groups within our working group, those that have different interests. So we want privacy interests represented, we want rights protection interests represented, we want law enforcement represented.

And that group - the task of that group would be to develop a list of questions for the data commissioners that would be very helpful for us to get responses on in Copenhagen. Now the idea would be this small group would come up with some proposed questions agreeing together among yourselves on the questions and then submitting those to the working group so that the working group can agree or not agree on the questions.

So what I'd like to ask between now and certainly by next Monday, for volunteers to participate in that group. And it'll be a short effort, probably

going to have a week or so to give something to the full working group so that we get it all done before the Copenhagen meeting. But please talk to your groups to see who you would like to represent you and submit that on the list this week.

And you can do it by constituency or stakeholder group, you can do it by interest area. The point is don't want to the group to be too big because it's going to be a short order task. So - and anybody that would like to participate can, but let's keep it small and not have a lot of duplicates. You can coordinate among yourselves for example if you're in the IPC as a person who would represent all of you, you can coordinate among the NCSG or whatever - however you want to do it, law enforcement people, you can coordinate among yourselves, GAC people.

So if you would do that please that'll be an action item so that between now and Monday we would like a volunteer from each interest area at least that will work together probably the following week in coming up with some questions. So our meeting two weeks from today the working group could consider the questions that you come up with. Shouldn't be a huge task but it's one that - it'll be helpful if there's some thought put into it. So that's an action item for everybody.

Looking at the agenda, so we have some action items. The - and the decision points that will be polled. Our meeting next week is on - at the alternate time. And we're going to continue this direction we're going right now and talk about the poll on purpose and we're going to have to - the leadership team is going to have to work through exactly how to proceed. We'll get back to you on that but we will be continuing this in our meeting next week and hopefully finalizing the group of volunteers. So please do that before that meeting.

And do it by Monday identify the volunteers from your group so make sure you have somebody on it that'll represent all of you. And that group will have about a week long task to just email and text and maybe even have a call that

staff will facilitate so that we can come up with some good questions for Copenhagen for the data commissioners to answer some of the struggles we're having and make sure we have a good understanding of the requirements certainly of Europe but I think it goes beyond that as Peter has pointed out several times.

Is there anything - sorry to talk so much on that - but hopefully we got a little bit of closure in this call. If - is there anything I have missed, something else we need to do on this call? And, Marika, I did see some of your private comments. I just haven't had time to respond, but you're right, we'll need to look at ICANN's mission, I think it was Peter that said we should look - somebody said we look at the ICANN bylaws and so forth. Absolutely true. We'll do that as we begin to proceed on this.

Not seeing any other items that we need to cover. Let me say thanks, good discussion. Keep it up on the list. And we will meet again at our alternate time next week. At this point I'll adjourn the meeting and the recording can stop. Thank you very much.

END