ICANN Transcription
GNSO Next-Gen RDS PDP WG
Tuesday, 07 February 2017 at 1700 UTC

Note: The following is the output of transcribing from an audio recording of the Next-Gen RDS PDP Meeting on the Tuesday, 07 February 2017 at 17:00 UTC. 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. Attendance may be found at:
https://community.icann.org/x/HIzRAw
The audio is also available at:
https://audio.icann.org/gnso/gnso-nextgen-rds-pdp-07feb17-en.mp3

Coordinator: The recordings have started.

Michelle DeSmyter: Great. Thank you. Well good morning, good afternoon and good evening. Welcome to the Next Gen RDS PDP Working Group call on the 7th of February, 2017 at 1700 UTC. In the interest of time today there will be no roll call as we have quite a few participants online today. Attendance will be taken via the Adobe Connect room so if you're only on the audio bridge would you please let yourself be known now?

All right thank you. And as a reminder to everyone please state your name before speaking for transcription purposes. Also please keep your phones and microphones on the way not speaking to avoid any background noise. When best I'll turn the call back over to Chuck Gomes.

Chuck Gomes: Thank you, Michelle. And welcome everyone to our call this week. This call is going to be a little bit different as we are focusing on data protection and that

will be a process to actually doing some deliberation on this call on data protection for collection of thin data elements. So we will start off a little bit differently.

But one thing that is still the same, let me give everybody an opportunity to update -- to share with us if they have an update to their statement of interest. Any updates please raise your hand. Okay not seeing any hands there, what it like to do then is bring up the slides from Peter so that he can give us an introduction of the - some of the data protection principles and issues that we've been talking about on the list for the last several weeks.

And after that we will let Stephanie also jumped in and share something with regard to data protection principles related to what we've been deliberating on on some key concepts the last few weeks.

So the slides are up and I will turn it over to Peter to let him go over those. Now we are going to let Peter go through all of the slides and then let Stephanie share her thoughts, and then we will have Q&A. So, Peter, are you on the call? I'm looking for Peter right now and I don't see him on the call. So let me ask staff to...

((Crosstalk))

Marika Konings: Chuck, this is Marika. Peter is there. He's actually in as a presenter in the Adobe Connect. We just need to make sure he's on audio...

((Crosstalk))

Chuck Gomes: ...scroll down to look at the bottom of my list so I missed that. Thank you. Okay Peter, sorry about that. I'm glad to see our list of participants is long but I was down at the bottom of it and didn't see you. So Peter, thank you very much for volunteering to do this. And I turn it over to you. Peter, are you on

mute because we're not hearing anything. I think his mic just lit up. Let's find out.

Marika Konings: No, that's actually not the mic. It's his symbol for speaking louder so, Peter, either you need to connect your audio via the phone symbol at the top of the Adobe Connect pod, or you need to dial in, or you can give us your phone number and we can dial out to you, one of these options. But at the moment your microphone doesn't look activated.

Chuck Gomes: I apologize. This is Chuck. We should have tested Peter and Stephanie's mics before we started the meeting. That's my mistake. So apologize for that. Stephanie, warning, if we are unable to get Peter's audio fairly quickly I may turn to you and see if you'd like to share your thoughts first, so just a little bit of a warning there. Hopefully we won't have to do that. Okay.

Marika Konings: This is Marika. I decide the microphone appearing that it has gone again. I don't know, Peter, are you on audio or...?

Chuck Gomes: If you can see the chat, Peter, they're willing to dial out to you if you give them the number to call.

Daniel Nanghaka: Daniel Nanghaka here for the record. I'll be on the audio connection. I won't be able to log into the Adobe Connect.

Chuck Gomes: And who was that?

Daniel Nanghaka: Daniel.

Chuck Gomes: Okay. Thank you Daniel.

Daniel Nanghaka: You're welcome.

Chuck Gomes: All right, let me turn to Stephanie. Let's test your mic, Stephanie.

Stephanie Perrin: Hi there. It's Stephanie. Can you hear me?

Chuck Gomes: I can, you're coming across loud and clear. Stephanie, would you be willing to share your thoughts while we are trying to get the connection with Peter fixed? Is that possible?

Stephanie Perrin: Well I can do kind of backwards because I was planning on supplementing what Peter was saying from the perspective of common law countries and other countries around the world, and just how the concept of purpose is instantiated in law in those countries and other jurisdictions. So, I mean, I can charge ahead, it's a bit backwards though.

Chuck Gomes: Go ahead. I apologize for doing that because I know I had said we were doing it the other order, I informed you and Peter of that so I hate to put you on the spot but at the same time we've got 40 people on a call and I don't want to just do that. Let me give Peter one more chance to say something just in case it's been fixed. And, Marika, go ahead. Are you on mute, Marika?

Marika Konings: It just takes me a second to get unmuted, to put in my code. I was just wondering maybe to buy some time, and I just saw the microphone of Peter appearing again so I guess he is trying to connect. But maybe I can give the update under Item 4 so we already cover that off and buy a few seconds or minutes to get Peter connected. Although I see again the microphone...

((Crosstalk))

Chuck Gomes: Go ahead Marika. So we are going to skip to agenda Item 4 and allow a little more time for Peter to connect. And then if that doesn't work we will go ahead and have Stephanie share her thoughts. Go ahead Marika.

Marika Konings: Thanks. Yes, we just wanted to give an update to the working group with regards to planning for the ICANN meeting in Copenhagen. So currently

there are two slots that have been requested before the working group. One on Saturday from two o'clock to a 4:45 local time, and the other when there is a secondary slot that's available on Wednesday from a 1:45 to three o'clock local time.

I think the current thinking is that the Saturday meeting would be similar to what the working group has done in the previous meeting, basically continuing its deliberations that having a larger slot available that will hopefully allow to cover a bit more ground.

There is, however, a secondary slot available as well so that is something for the working group to consider whether you want to use that slot either to continue the deliberations from the Saturday session whether there's another purpose you want to consider for that meeting, for example, you know, briefing that community on where things stand or another option as well as data protection commissioners are participating and, you know, should they of course be still available Wednesday as well to have a dedicated session with some of them to go through some of the questions that the group may have.

So that's where things currently stand. This is of course still a draft. You know, the schedule hasn't been published yet so there may still be changes but maybe for now you would like to just pencil back in and take note of that for scheduling purposes.

Chuck Gomes: Thank you very much, Marika. Any questions on that? Just to get an idea, how many of you, if you could just put a green check in the chat if you're planning on -- you're definitely planning on attending in person in Copenhagen? If everybody would just put in green checks if you're - I guess I better do it too, I'm saying that. Okay.

Good number of participants. Of course as always there will be remote participation if you are unable to attend in person. And the hours may not be

great for some but good, looks like it's going to be a good turnout. I hope that those who can't attend in person will participate remotely so that we have a good turnout there. Alan, go ahead.

Alan Greenberg: Thank you. Just wanted to note that I will be in Copenhagen to whether I will attend a meeting or not is not clear due to conflicts. By scheduling them in the middle of the - within the working week of ICANN you're effectively saying anyone who has other commitments in other ACs, SOs, probably cannot participate or cannot participate fully. So just so people understand. Thank you.

Chuck Gomes: Thanks Alan. Okay please remove your checks so that we have a clean slate there. All right so Peter, if you're able to speak please speak up, otherwise we're going to go to Stephanie. Okay Stephanie, sorry to do this to you and I know it's not ideal but I appreciate your flexibility in being able to jump in.

Stephanie Perrin: Okay. Not a problem, Chuck. I mean, basically you will find this rather repetitive because I've been making these points in the chat probably with nauseating repetitiveness to some folks. However, here we go.

Basically one of the basic principles of data protection law is there is a general requirement pretty well everywhere and a 109 laws that we have around the world that processing be fair and lawful. And the issue of course boils down to what does fair and lawful mean? And fair really is interpreted as meaning that there should be limits to the collection of personal information and that those limits should be focused on the purpose.

In other words, while any amount of information is interesting to a data processor or a data controller, that doesn't mean that just because it would be useful you are allowed to collect it. Now in the context of most common law countries, and I think in the United States, there has to be a legal mandate for a government department to collect data.

This gets much fuzzier in the private sector because public-sector you can easily say that if you're with the Transportation Department and you're issuing drivers licenses, that the data that you gather for the purpose of issuing a driver's license have to be directly related to the issuance of that license and intrusion into the private licensed individuals is not necessarily tolerated.

When it comes to private sector companies that are offering a service that is not mandatory, let's say something like Facebook for instance is a great example, basically they can define what the user experience is and what data they think is relevant and state those conditions.

And in the United States after the Internet, the concept of notice and choice became kind of the rule in the United States and because of that it has spread over the Internet. You have to tell people what you're collecting through your notice and they have a choice that is supposed to be issued by a consent. And in many, many cases of Internet services, that is a consent that can be kind of take it or leave it. You know, if you want the service you agree with this. We're all familiar with this from our - I'm thinking of my Apple contract which is something like 80 pages.

So having said that, the restriction of the collection of data to that which is necessary specifically for a purpose is a key focal point in data protection and therefore defining the purpose is fundamental. And I maybe saying something that Peter is going to say here, but the data protection commissioners of Europe and of the International Working Group on Data Protection and Telecommunications, which I would guess is an international group, it's not just the EU guys, they have written numerous times saying please specify the purpose of collection. And ironically so have the SSAC written, please specify what the purpose of collection is.

So in many respects, security people have similar concerns to data protection people because the collection of information involves...

((Crosstalk))

Peter Kimpian: Hello? Hello? Oh.

Stephanie Perrin: Hello?

Peter Kimpian: I hear my voice.

Stephanie Perrin: Wonderful. Am I ever glad to have you back. Now would you like me to stop and let Peter jump in here?

Peter Kimpian: I let you finish maybe.

Stephanie Perrin: Okay, all right so I will carry on. So basically the way this has been sorted, and it's important to understand that between the civil law and the common law there are certain differences. Also when you're evaluating data protection law internationally you have to look at a number of things and one of the key documents that you have to look at is the Constitution where the protection is the constitution where the protection is against unreasonable search and seizure are usually spelled out.

And any charters of rights that may or may not exist. In Europe, obviously there is a fundamental charter which Peter is going to talk about. In Canada we have fundamental charter. That's not necessarily the case in, for instance, all of the Asian privacy laws. And I'd refer you, if you're interested in how this sorts out, internationally to (Graham Greenley)'s excellent book on Asian data privacy laws where he looks at a series of laws in comparison to see how they translate in fundamental principles, many of which came originally from the OECD guidelines.

So what we did in Canada was we basically went in the private sector legislation, as I say in the public sector legislation there has to be a legal - a

law that authorizes you to gather certain data. And you have to play within the laws. But in the private sector when the private sector law was drafted it was basically followed a variant of the OECD guidelines, mainly that Canadian standard that says you have to be accountable for your data collection; the purpose must be limited.

That you need to state that in your notice. And then when it hit Parliament, the clause was added that the purposes have to be what a reasonable person would think was appropriate under the circumstances. Now the reasonable person test is a pretty well-known test, it's called the man in the Clapham omnibus, basically what would the average person think was acceptable under the circumstances for you to gather.

So keep that in mind, what does the man in the Clapham omnibus think is appropriate for ICANN to designate should be gathered for these purposes. What is the purpose of ICANN, in other words, in a gathering of personal information?

So I think a lot of the confusion that we have been experiencing, in my view, is the fundamentally different way that they Peter and I are looking at the expression of purpose to potential uses of personal information. We are not arguing basically that these potential uses are not useful, they're not relevant, they're not appropriate in certain circumstances. But that potential use for other purposes, we would call them secondary purposes in my jurisdiction, is not a sufficient reason to include it as the purpose of collection. These are subsidiary purposes.

So I think that's probably enough for me. I would be certainly very happy to answer any questions on this. And if I haven't gone into enough detail I'm happy to jump in and give further detail. Thanks.

Chuck Gomes: Thanks Stephanie. I saw Susan's hands or checkmark. I'll come back to you. This is Chuck. So I'll come back to you after Peter does his presentation and

then we will open it up to the whole group for Q&A. So you'll get a chance to follow up on other points after Peter does his presentation. So, Peter, welcome. Sorry for the technical glitches. Please share your thoughts and your presentation.

Peter Kimpian: Yes, yes, thank you very much. I'm very happy to be on the call and it's my mistake, I may be messed up something. My mic said it's on but obviously you could not hear me. But now I think you can hear me.

And I just want to run quickly through the slides I prepared and to highlight some of the issue. I thought it might be relevant for the discussion, which is ongoing on the RDS PDP. But first I would like to start from a global perspective.

As I, certainly coming from a Council of Europe and from Europe as a continent, that privacy is not a European issue anymore. We see it as a global one and not only me but all privacy professionals, and not only privacy professionals by professionals.

I had a chance to speak with (unintelligible) privacy as a global issue and certainly we have differences in our legislation is, maybe on the articulation of rights to privacy and moreover on the execution and the enforcement side. But I would like to stress that the right to privacy is a universal human right. It is declared by Article 12 of the Universal Declaration of Human Rights, and Article 17 in the International Covenant on Civil and Political Rights.

It is very important to know this at the global level because human rights are designed, I mean, in legal system, are designed differently and have different mechanisms -- legal mechanisms as the articulation, for instance, of a state interest.

Normally we have, globally we as nations of the world or people of the world, and after the second world war we have invented the Universal Declaration of

Human Rights to stand above the whole legal system. So being said that, I would not go too much into details.

Of course we have regional text, regional conventions. In Europe this is convention (unintelligible) which is not only for Europe because there are third parties, third countries who are also joining it as it is an open convention. But for instance, my presentation I use also as reference the APAC policy framework and the OECD policy framework as well as the European Union regulation and legislation on privacy.

So being said that, let's move on to the main principles. There is one principle I would like to start with and to really put the emphasis on. I think if somebody understands this it will understand a lot of things about data protection and privacy. So the issue is you can find on the last upper side of the slide that individuals have to be in control of their personal data which means the whole trail of data.

So I, as a person, have to know and have the right to know what is happening to my personal data everywhere, I mean, in every reach of the data processing activities whomever are making it or are processing it. There are some overarching principles as well comment the necessity proportionate and the purpose specification, or we can call it purpose limitation principle, I know we have discussed this in its PDP RDS a lot and there are very good material already in the wiki for this so I will not spend too much time on these principles.

But I would like to go through more specific principles and may be to take an example and to showcase on the example how it works in practice because all these principles have some consequences and some legal implications for procedures.

So the first one is legitimate aim or we can collect legitimate purpose. So for data processing we have to have a legitimate right or legitimate purpose. It

basically comprises all the following principles which starts by lawful and fair means of data processing.

Wild if we take the example of the online marketing, and I will try to demonstrate through this example those principles, so what does it mean, “lawful”? That it has to be regulated in a legal text or at least it has to be or in other jurisdictions it has to be - there is a requirement not to be banned or not to be, how to say, forbidden by the legislation.

So is the online marketing is not bound by any of the legislation? As far as I know it is not bound so it can say that it is lawful. What does that mean, fair means of data processing? So for example, if we are thinking about the means of data processing, so for instance gathering phone numbers of data subjects for data processing, for marketing purposes, is this legal? Yes, we said that it’s already legal but that means how we do it can make a lot of difference.

So if we are, for instance, making phone calls at 10 o’clock in the evening or if we are taking those phone numbers from other than public sources and that can mean unfair means of data processing.

There is another very important legal basis is the valid legal base which can be low consent contract vital interest of the individual. And it is so not only in the European legal text, it is the same - same provisions can be found in the APAC privacy framework or the OECD privacy framework. So we have to have a legal base to process this personal data out of which consent is one, but not the only one.

There are some other very relevant principles as to the (unintelligible) and relevance -- and the non-excessive of nature of the data processing and the data process. And of course there is the obligation for the data controller to keep the data accurate and where necessary up to date.

It also there is what we call the last principle, I would like to refer to the data minimization principle is basically saying or let's put it bluntly, forbidding the (bar) processing of data.

So we are not processing data for the sake of it because if it's fun and we have means for doing it, but we are processing it for a reason, for a purpose. And during the processing of the data we have to, I mean the data controller has the obligation to process the minimum amount of data which is fit for the purpose.

So passing through the principles, there are of course exemptions to this data, also to the principles but also to the provisions, the data protection legislations provisions. So exemptions, as you can see on the slide, are from the purposes of state security, public safety, monetary interests of the states and suppression of criminal offenses.

And there are others as well as protecting the data subjects or the rights and freedom of others and the statistical and research purposes. So these are the classical exemptions where the data protection principles, the data protection rules are not in its entirety applicable because usually this is the philosophy behind it. There are higher interests, the interest of the society or the interest of the state behind those exemptions. So for the state security is a good for everybody, is a common interest for a society.

But being said that, as I was referring to the difference between interest and human rights, we have to make a balance at least in some part, in some way in all the countries I know jurisdictions have come out with the same results, whether you call it as reasonable expectations or you call it as data minimization or purpose limitation principle, there is always conditions to use these exemptions.

So because there is the underlying reason for this because the processing of personal data for these purposes, it namely national security purpose, law

enforcement, etcetera, can constitute an interference with this human rights so it's obvious that it infringes those human rights. So we have to establish a criteria under which they are permissible or they can be done.

So with this, I would like to come to the disclosure of data. We use different definitions for the same phenomenon, disclosure of data, third-party access to data, we use -- or we use to use it in Europe for European legislation and now we attempt to use it for the data processing.

So for this, as Stephanie also referred to secondary purpose of data, this is the Canadian definition. We say that the same rules as for the processing applies, which means that we have to fulfill or we have to -- a data controller has to fulfill the whole -- the principles for data processing and the provisions prescribed by the law for data processing.

However, in this relation there is a third party who enters into the picture. And there is a second purpose because for the same if we would process the data for the same purposes that will not be secondary purpose so that will not be a further processing of data or disclosure of data as we can -- as we would say. But there is always a secondary purposes for this kind of processing the activity, but this is not - it will not be for the data controller, the original want to define these purposes but for the data controller who is asking for this purpose.

The original data controller is usually - defines the conditions and the procedures under which it can disclose the personal data and for this it has to undergone the same test whether if they comply with the principle of data processing or not.

With this, I will arrive to my conclusion and the last topic I wanted to raise today, this is the question of accountability. So you can see on the slide there are - in every each of the texts, legal texts I was referring to, there is a mention of accountability and all the texts are - legal texts are requiring data

controller to - or holding data controller to be accountable for the use of the data protection principles during its operation.

But being said that, we can conclude, if we come back to the previous slide I tried to explain that the collection of personal data for a specific purpose would remain responsibility also for the implementation of the data - of the privacy and data protection purposes for that purpose. So one data controller has always bear this in mind whether if it's a private one or a public one. But these are the main principles that we normally we cannot defer from because it is prescribed by law and it is prescribed basically everywhere in every legislation I know or I am aware of.

So we have to deal or take this into consideration and to really think about this issue when we are discussing about the purposes. It is good to enumerate purposes but we have to also bear in mind that the organization or the data controller whether if it's ICANN or registrars, registries, that maybe we can discuss it later but the data controller as such will be held or, yes, will be held accountable for the data processing under these purposes, which means all the principles that I have enumerated in the beginning which is - which goes from lawfulness to the fair means and the accuracy and the up to date nature of the data and so on and so forth.

So with this, I would like to conclude my presentation by saying or by repeating that Council of Europe would like to facilitate a high level meeting on the 13th of March during the Copenhagen meeting where those kind of issues would be debated or we hope that it would be debated in a higher - in a high interest topic during 13th of March.

But we are also working on bilateral meetings of the participants to this privacy meeting with the interested communities or interested groups within ICANN to start to debate or start a dialogue on these issues and to have a better understanding not only for you how privacy principles maybe work or

are interpreted in - by authorities or by legislators in different parts of the world but also for us to better understand how ICANN work.

So with this I will thank you for the opportunity. I'm open for any questions you might have.

Chuck Gomes: Thank you very much, Peter. We'll get a chance to - everybody will get a chance to ask questions shortly. But, Stephanie, let me give you an opportunity to follow up with anything additional you'd like to add before we go to Q&A.

Stephanie Perrin: Thanks, Chuck. Stephanie Perrin for the record. I think probably Peter's probably well-covered it. Let's see how many questions we get in view of the time. Thanks.

Chuck Gomes: Okay. Thanks, Stephanie. Chuck speaking again. So let's open it up for Q&A. Please raise your hand or in the case of Samuel you'll have to speak up if you want to get in a question or a comment. And let's take as much time as we need to get clarification on the things that Stephanie and Peter have shared because all of these things are going to become very relevant as we deliberate on the questions, sub questions that we're going to ask with regard to data privacy and - data protection and privacy. So please raise your hand if you have a question. Susan, you're first.

Susan Kawaguchi: Thanks, Chuck. Susan Kawaguchi for the record. And thanks, Peter, that was very informative. So I'm wondering what of the information you provided today pertains to commercial entities?

Peter Kimpian: Shall I answer directly or...?

Chuck Gomes: Yes, thanks, Peter. I should have said that. I would like you and Stephanie both to respond as you feel comfortable to the questions. There's no need for me to get in the middle of that. So just go ahead, just identify yourself -

probably everybody will recognize your voice now. But identify yourself and share the response.

Peter Kimpian: Right. So this is Peter. The first part of my presentation goes basically for all of the - all type of data controller whether it's private or public. The second part, I mean, the exemption part I would say like this goes mainly for the public one. But I included it in here to demonstrate the logic according to which they are - the legislation are designed for those purposes and to understand how narrowly or restrictedly are usually legislated when it comes to purposes pertaining to national security, public safety and so on and so forth.

Susan Kawaguchi: So - and I just have a couple follow on questions here. And...

Chuck Gomes: Susan, remember to identify - everyone remember to identify yourself. I know your voice well but some people may not.

Susan Kawaguchi: Yes. Susan Kawaguchi for the record. So a commercial entity would have the same right to privacy of their data as, you know, myself as an individual if I was...

Peter Kimpian: Oh.

Susan Kawaguchi: ...working in, you know, living in Europe.

Peter Kimpian: Yes, no, I'm sorry, maybe I didn't get your question at first. But, no, no so privacy is a private - it's a human right so which are linked to humans so to human beings. There are discussions and I'm open to have - to share my views on this as well. There are discussions whether a private entity should be enable to have the same rights as natural persons. But for now in jurisdiction I know, privacy is a human right which only applies to human being.

Susan Kawaguchi: Okay, that's really helpful. And then I posted - I pasted in Facebook.hu's registration data record in the chat - the formatting is pretty, you know, doesn't work very well. But I was wondering how Hungary defines purposes for collecting and displaying of registration data. If your country has gone to that work and defined those purposes, then that might be helpful to, you know, inform our discussion. I was wondering if you could talk about that.

Peter Kimpian: I'm sorry, I haven't heard very much. So can - I'm sorry, can you repeat the question because...

((Crosstalk))

Susan Kawaguchi: Sure. So I was just wondering for dotHU, which I think is your home country, right?

Peter Kimpian: Yes.

Susan Kawaguchi: ...Hungary? So if...

Peter Kimpian: So, yes.

Susan Kawaguchi: ...if the registry has defined purposes for collection and displaying in your own home country that would comply with these laws. If they have - if they've gone to the work of actually defining the purposes, is that something you can speak to? Is that something you could share with us because that might help inform our discussion.

Peter Kimpian: Well, I'm not at all there about all the - all this issue. So I'm - I have to inform myself on this because I really don't know how they - how they worked in the past on this.

Susan Kawaguchi: Well, do you feel like your country is in compliance?

Peter Kimpian: I cannot - I cannot - I cannot comment on this. I mean, first, I don't know how dotHU is handled, and second, I'm not representing neither Hungary nor any other organization than the Council of Europe and we - so I don't know simply. And personally, to be open and honest, I don't know if they are compliant or not.

Susan Kawaguchi: Okay thank you very much.

Chuck Gomes: Okay thanks, Susan and Peter for that dialogue. Remember to say your name every time. This is Chuck, by the way, I have trouble doing that too. Most of us are learning each other's voices on our live calls but when you read a transcript that doesn't help. So please try to do that.

Now before I go to Alex, I want to confirm something that I think I heard in the dialogue that just occurred, and that is that the privacy principles that you talked about, Peter, in your presentation and that Stephanie talked about, they apply to - is it correct to say that they apply to personally identifiable information to what we call PII, and not to other types of information? And, Peter and Stephanie, you can both respond to that. And you'll note that there's been some discussion of this in the chat as well.

Peter Kimpian: My short answer - this is Peter - my short answer would be yes.

Chuck Gomes: Okay thank you.

Peter Kimpian: As I already saying that human rights are applicable to humans so PII only applies to personally identifiable information.

Chuck Gomes: Okay and for those that are concerned about our restriction right now in talking about thin data, we're going to get specifically - we're going to specifically look at thin data as we proceed so bear with us please.

Peter Kimpian: Yes.

Chuck Gomes: Alex, go ahead.

Alex Deacon: Yes, hi, Chuck. Thank you. This is Alex Deacon for the record. Yes, so thanks, Peter, for this. I think it's very helpful for me at least as I'm definitely not an expert. I wanted to chat about exceptions, and I understand and agree with the need for the proper balance and proportionality. But specifically I'm curious about the exception that allows data processing for the rights and freedoms of others. I'm curious as to your thoughts kind of generally about that specific statement.

But I think more generally I'm curious how should these exceptions inform our discussions in this working group? Should - how should we be taking these exceptions into account when determining not only the purpose but also when we get into the details of what data should be collected and how it should be processed and when and if and how it should be disclosed. Thanks.

Chuck Gomes: Peter, would you like to respond to that?

Peter Kimpian: Yes. Yes, this is Peter. So this is one of the beauty of the human rights law and human rights legislation, so for instance there are two informational rights which we call the informational rights, right to privacy, right to data protection and freedom of expression. We have thousands and thousands of pages of case load on this how, for example, the Court of Justice here in Salzburg define the way of making a balance because those are in situations are contradicting rights because if something is public then it's not private anymore. So how you can - how one should decide whether if it's - if I disclose if I don't disclose or if I make it public or I don't make it public.

This is, I think, because I'm a lawyer, and I tend to listen to what courts are saying as they are very vocal and getting more and more importance on these issues, I would use those cases. We have cases like in Europe of High

Courts, Salzburg Court, but even the Luxembourg Court can be also of use on this issues. But we also have the US High Court and several US courts.

And these are the two main jurisdiction I already learned about, I would say like this. But I would be happy also to know more about maybe Canada. We have this or other part of the world. But I think that the solution jurisdiction - the caseload can give we cannot list too much, I mean, if we follow them because at the end they will judge the specific cases if there are any.

Chuck Gomes: Thank you, Peter. This is Chuck again. And before I go to Stephanie, I'd like all of you to note any questions you have, not only for the meeting today but hopefully in Copenhagen we will have opportunity to ask the data commissioners there some very specific questions to get the clarity that we need. So please keep a record of those so that we can compile that in preparation for our meetings in Copenhagen that Marika mentioned at the beginning of our call.

Stephanie, it's your turn.

Stephanie Perrin: Thanks very much. I just wanted to clarify this matter of commercial versus personal data. It varies by jurisdiction whether the employees of a company are considered to have rights with respect to their data protection on the Internet in particular. And for instance, in Canada, we consented to a carve out for business card information. I think unfortunately because it's rather a huge carve-out.

Various jurisdictions have come up with whatever is required. You will notice that in the early document sent to us by the data protection commissioners on this topic, they have pointed out that in, for instance, Germany, you have to seek the consent of employees before you put their name and phone number up on the Internet public registries.

So we have to remember that the employees of companies have personal information rights, at least at a high level if not in the letter of the law. And that there are other human rights that are implicated with respect to small groups and organizations that are registering a domain name. So a lot of the argument that took place in the PPSAI with respect to the small organizations being able to use privacy proxy services, is they don't have the means to hire lawyers or whatever to protect their data and that exposing the data of employees may expose them to risk.

So that is a different right that is specified in the constitution. And I didn't go back on that but, I mean, the sorting out of what ICANN has to do with respect to personal data and data of identifiable organizations and individuals rests not entirely on data protection law, it also rests on other human rights law and constitutional protections. So I just wanted to point that out. I see Steve has a question and I'll read it and respond later if that's okay. Thanks.

Chuck Gomes: Stephanie, go ahead and read it and respond right now if you'd like. This is Chuck.

Stephanie Perrin: They may or may not be data protection rights, depending on which country you're in and how exposed you are. So for instance, if I am the secretary of a small church somewhere and I'm running the Website and I am the person that unwittingly registers the domain name, and then I discover that my home address and home phone number are exposed on the Internet, that would be my personal information particularly if I'm a volunteer.

So and in most civil society organizations, such as churches, synagogues, political groups, these people are volunteers. So that is personal information. And I think one of the problems that we face getting back to that whole issue of notice and choice, the problem with notice and choice is nobody likes reading Apple's 80-page legal agreement nor has the concept of short notices, which was put forward by (Hunton) among others, really succeeded

because you lawyers will say, well a short notice just doesn't give enough legal notification of what's going on.

So when it comes to ICANN and the notice that is required by registrars to inform individuals of what their data protection rights, I don't see anything on my registrar's Website that informs me of my data protection rights. I don't see it in my contract and, you know, I just haven't got around to complaining yet. So, I mean, these are issues that we have to bear in mind the notice requirement is going to be pretty extensive if we start looking at that. Thanks.

Chuck Gomes: Thanks, Stephanie. Chuck again. Susan, go ahead.

Susan Kawaguchi: Susan Kawaguchi for the record. Stephanie, I have no interest, you know, I mean, I'm not - I don't think we need to make it extremely difficult for mom and pop businesses, and I think we can, you know, there is proxy registrations, there's some avenues and we could build a stronger protection for them. But I do think this group has a duty not to convey individual human rights, personal rights, to a commercial entity.

Facebook doesn't deserve that protection. And we don't ask for that protection. I don't think, you know, and, you know, yes it's a little bit of a gray area, where you go from somebody like Facebook and Google all the way down to somebody, you know, acting as registrant for their church, I think somebody used this one, as their church, you know, domain name.

But I think that we can't keep having this discussion without realizing we have two, at least, there could be more, complete groups of data that cannot be treated the same. So, I mean, that's just my point of view.

One question I had for you also because - and it's similar to the question I asked Peter - was I think there's some value out there in the ccNSO that we haven't sort of leveraged yet. But I was wondering if dotCA, CIRA, has - the registry has defined purposes for collection and display of the registration

data for a dotCA, because they definitely make a difference between a, you know, an individual's domain name and a company domain name or a commercial entity domain name. So I was wondering if you had any perspective on that, what CIRA - how CIRA defines those purposes.

Chuck Gomes: This is Chuck. Stephanie, if you'd like to respond if you can, that would be okay.

Stephanie Perrin: I haven't checked on CIRA's current privacy policy. I would like to point out that there is considerable confusion, in my view, in the data protection commissioner's community as to the differences between the ccTLDs and the gTLDs. Number 1, they don't understand that - I shouldn't just say blanket "they" but I think there are plenty of data protection commissioners who have not dealt with complaints.

If you haven't dealt with complaints and you haven't been approached by your ccTLD to assist them in developing policy, and I would say that's an abnormality when the ccTLDs reach out, then you're likely blissfully unaware of the arcane nature of how domains are allocated on the Internet. So they can be forgiven for not understanding the distinction between the ccTLD rules and the gTLD rules.

Now, secondly, I mean, I did the first CIRA policy and I was appalled that they wanted things like a passport, but there is a requirement in Canada that (unintelligible) have a Canadian (unintelligible) in order to get a - or there was at the time - in order to get a dotCA domain. So obviously it's much easier if you're a company. There are certain requirements. And if you're an individual then you have to prove your Canadian existence or you did. As I say, I haven't checked lately. I know they've had several revisions.

So I think that I would just like wave a flag of caution. If we look at the ccTLDs some of them have good practices, others have practices that are quite difference, in other words, if I'm just registering a gTLD and there's no

requirement for me to identify my nationality, then I'm not going to produce a passport. Am I making that clear? Thanks.

Chuck Gomes: Thanks, Stephanie. So before I go to Maxim, hopefully it's clear to everybody, and I think we all knew this before we started, that there's lots of variation depending on what jurisdiction we're in. Secondly, I want to say I know we're at a very high level right now, we're - and let's realize that and not get too worried about that. We're going to have to, as we deliberate on specific data elements we're going to have to - I think it'll be easier for us to answer some of the questions that need to be answered. So we will get there so bear with us as we do that. Lots of good discussion in the chat, lots of good questions raised in the chat.

When we get into specific deliberation of data elements, and I hope we get to the thin data elements today, certainly going to try to do that, it'll be easier for us to get - try and reach some resolution on what recommendations we will make. And obviously those are going to have to vary by jurisdiction and it's not as if we're going to cover every jurisdiction in the world individually; that would probably be impossible. But so bear with us on this.

Now I want to, before - again before I go to Maxim, there was some - and you may need to scroll back in the chat if you didn't read it, but Alex had asked a question in the chat about who data controllers are, and you heard Peter use the term "data controller." Stephanie gave what I thought was a very helpful definition of - or not a definition but rather illustration of who the data controllers are, ICANN being one, registries and registrars in a different sense and in other cases they're data processors.

So if you didn't see that exchange between Alex and Stephanie, look over the chat later or scroll back up there now. I thought that was very helpful because I think the term "data controller" is going to be a very important one as we move forward. So please take a look at that if you didn't see that.

Maxim, now I'll turn it over to you.

Maxim Alzoba: Maxim Alzoba for the record. (Unintelligible).

Chuck Gomes: What was that? I didn't hear.

Maxim Alzoba: Okay. Maxim Alzoba for the record.

((Crosstalk))

Maxim Alzoba: Do you hear me?

Chuck Gomes: Yes.

Maxim Alzoba: The question is there is no formal method of distinguishing the fields which constitute personal data from the fields which do not right now. Do we need to review possibility of production of special flag of some kind saying that this particular set of (unintelligible) constitutes personal data or not? Thanks.

Chuck Gomes: Thank you, Maxim. And that's something we could decide to do. I don't think we can answer that question right now. But one of our requirements could be something like you're suggesting, maybe it won't be. But that's certainly an option for us to consider and we're going to have to look at that because one of our responsibilities will be to design a system, if there is a new system, that would properly comply with data protection law in various jurisdictions.

So keep that in mind. That may be an implementation issue that we have to deal with later on. Theo, your turn.

Theo Geurts: Thanks, Chuck. And this is Theo for the record. So the last hour I've been hearing a lot about fundamental rights, privacy issues, privacy laws. And I'm - this is more of a comment than a question actually. (Unintelligible) the feeling here that when we actually going into these deliberations I think we actually

should be sort of using privacy by design to enter those deliberations because I have the feeling that we have a lot to talk about but we are not laying a sort of fundamental layer on which these discussions should be based on.

And from what I'm seeing that ICANN can be held liable or is the data controller, I'm getting pretty nervous there. End of comment. Thank you, Chuck.

Chuck Gomes: You're welcome, Theo. And I think I share the nervousness. It's not a black and white issue. If nothing else has come across in this session I think that's one of the key points. So we're going to have to deal with that. And it's not going to be an easy task but I think we're starting to lay a foundation that will help us hopefully remove some of our nervousness, although it may never go away totally.

So the - I want to make - at least get - I think we have at least in the chat had some good clarification in terms of what data controller means and it may vary in terms of the particular data as Stephanie described in her chat comment. I think we've identified that we're talking about personally identifiable information, although what we're going to have to decide is what is personally identifiable information for particular data elements.

So the question I have for Peter and Stephanie first, but then open it up to discussion for the whole group, is are there any of the thin data elements, as we've defined them over the last few weeks, considered personally identifiable information?

Peter Kimpian: Well this is Peter...

((Crosstalk))

Stephanie Perrin: Can I jump in here? It's Stephanie. The use of the term "personally identifiable information" is, in my view problematic. I realize it's come into common parlance; it's a US-based expression. But it, I think, seeks to avoid the problem of identification.

So a small subset of thin data that appear in - appears in a public registry may not be, in quotes, personally identifiable because there are no - there's no name, there's no address, there's no phone number. But if it is traceable through some other thing, back to a registry that connects that data with the individual, then it is - whether it is generated, and we had quite a heated discussion on the chat about this or whether it is gathered from the individual, it's personal data in that it refers to an individual.

When I used to argue about this in governments, I always used the line, and I am sorry to abuse the FBI, but that's what I used to say; if it's good enough for the FBI to arrest me then it's personal data. I mean, if a time stamp links me to an action, which can be detected through my, I don't know, credit card, to find me, and I get arrested because of that, that is still personal data.

So this is not to say that you can't release it. This is where I got really frustrated with this discussion on, you know, the collection, use and disclosure. We may all agree that it is reasonable to expose a subset of the data. But if the data linkage is there, then it is still personal data. And this has become more and more an issue as we look at the Internet of Things and the data that we generate by, you know, our appliances.

You know, my refrigerator is not personal but if I'm the only one in the house and the refrigerator is talking about what I just put in it, then those purchases are linked to me. So, I mean, these are important distinctions from the perspective of human rights and the application of data protection law.

So, I'm not trying to stop disclosure of thin data, which is something I think folks thought I was trying to do. I'm trying to get intellectual clarity about what this stuff is.

One example, if I can cite it to you, that has me sort of - me and my legal counsel banging our heads on the table was a government example where there was a - two filing cabinets side by side, one with all kinds of personal information about a particular native population and another with data that had been de-identified.

And it required a deputy minister's letter to link the very sensitive health data with the identity of the individual, therefore, the health data was considered not to be personal information. Now this is a distinction that the man in the Clapham omnibus would know is wrong. This is the kind of sort of legal (unintelligible) we get to in these discussions. Thanks.

Chuck Gomes: Stephanie, so you would use the term "personal data" instead of PII? This is Chuck.

Stephanie Perrin: Yes. It's clearer.

Chuck Gomes: Okay, that's fine. I just want to make sure I got that right. Now...

Peter Kimpian: Yes.

Chuck Gomes: ...the basis for my question on whether any thin data elements are considered personal data, I'll say persona data now, okay, would you consider any of those elements personal data? And the reason I'm asking that is I - we need to decide what data is impacted by the data protection laws in whatever jurisdiction we're doing.

So let me ask you, would you consider any of the thin data elements that we've been looking at as personal data? That's to you, Stephanie.

Stephanie Perrin: Sorry, I was on mute. This is Stephanie again. I would think that anything generated about my domain name that I registered as an individual could be considered to be personal. I mean, I would need to look at those data elements that are up there.

Chuck Gomes: So if we - this is Chuck again...

((Crosstalk))

Chuck Gomes: If we take that approach then you would consider everything personal data.

Stephanie Perrin: Well...

((Crosstalk))

Chuck Gomes: In other words, everything has to comply with the data protection laws. All data elements.

Stephanie Perrin: Right. Right, and that solves - I know that solves like it just throws you right in other volcano, but actually no. I mean, then you start sorting out, okay, which data is it reasonable to ask be disclosed in the concept of a - of getting a domain name. I mean, we got into this, unfortunately, unbeknownst to me, I used an expression that had come up many, many years ago in the debate, the idea of a driver's license. And Fab will recall seizing on that.

But, I mean, there is a certain amount of data that you recognize you have a public responsibility to disclose. And that's, I would argue, what we should be putting out in the thin data.

Peter Kimpian: This is...

((Crosstalk))

Chuck Gomes: Okay, Greg has been - this is Chuck. Greg's been very patient so, Greg Aaron, you're up.

Greg Aaron: Thank you, Chuck. This is Greg. I think Stephanie is talking about a really slippery slope here. I think she's talking about two things, and you can correct me, Stephanie, there's - you're saying that everything is personally identifiable but you're saying that there are circumstances under which some of that might be revealed. But what I see, after reading some of these data protection laws, is that some of - it sometimes depends on circumstances.

Like IP addresses are not always personally identifiable. And that depends upon a set of circumstances. But what I do see is that the European ccTLD registries publish thin data. And they have gotten that collection and publication vetted six ways to Sunday. And they all do it.

And you - you can't say it depends but then we see the practice, which has obviously been vetted by a bunch of people. Now ultimately - this is directed towards the leaders of the working group - I don't think this group is going to be able to proceed very far without some professional legal advice.

We can talk about it amongst ourselves, but at some point we're going to have to get some legal advice on some of these questions just as the thick Whois working group did and just as the EWG did. And we ought to perhaps be reusing and revisiting some of the advice that the EWG did if it's duplicative.

But what I hear Stephanie saying is it seems like a slippery slope and it doesn't necessarily seem consistent with what I've read, although I'm not an expert, I have to say, and doesn't seem to fit with what I see out there in the industry going on especially in the ccTLDs. Thanks.

Chuck Gomes: Thanks, Greg. This is Chuck again. Peter, I'm sorry, you started to talk a long time ago and I never did get back to you. So please, jump in.

Peter Kimpian: No, I'm - thank you very much. This is Peter. So I - this is a crucial question. So you heard me about how to interpret or how to - what are the articulation of some of the European legislation. So for this let me borrow the - and some thoughts for - some thoughts from other jurisdictions the APAC framework - APAC privacy framework.

So it says, because it defines the definition of personal information, which means any information about the identified or identifiable individual. And it - let me just read the explanation because there is an explanation attached to it. It will take two minutes but I think it's worth to listen to it.

The principles have been drafted against a background in which some economies, because it's basically centered on economic cooperation, have well established privacy laws and/or practices while others may be considering the issues. Of those with already settled policies, not all treat personal information in exactly the same way. So some, for example, my draw distinctions between information that is readily searchable and other information.

Despite these differences, this framework, the APAC privacy framework, has been drafted to promote a consistent approach among the information privacy regimes of APAC economy. This framework is intended to apply to information about natural living persons, not legal persons. The APAC privacy framework applies to personal information which is information that can be used to identify an individual. It also includes information that would not meet this criteria alone but when put together with other information would identify an individual.

So this is a possible response to it, I mean, to the questions. This is, again, a regional cooperation framework. It's based on an economy. So it's not exactly

ICANN context, but I think we can have some inspiration from this text or from other texts. We also have a recommendation - the Council of Europe just published the recommendation on data protection issues on big data environment where it is way, way more difficult to find out what is the personal data or what is not in a big data context.

But also for this ICANN, I can provide with this recommendation and we can have or the group can have inspiration from those texts I think. Hello? Every - anybody there? Hello?

Chuck Gomes: I'm sorry. I was on mute.

Peter Kimpian: Okay.

Chuck Gomes: So if you would send that, Peter - thank you very much. If you would send that definition to the group that would be much appreciated. Now to me, the way I understood that, it's pretty broad and kind of confirms that Stephanie was saying that personally - personal information covers just about anything if it can be connected with some other things to identify somebody.

That's not very helpful for us, as I think Greg kind of pointed out, that puts us in an awkward situation. So maybe what we should be asking, and I'm throwing this out for discussion, maybe what we should be asking - what we need to focus on is not whether data is personal or not, because it sounds like anything could be defined as personal, although we need to make the distinction with commercial organizations, with legal organizations.

Is we're just going to have to look at each data element, I think, and decide whether it can be collected, whether it can be disclosed and Stephanie indicated that she's not arguing that these - this information can't be disclosed because it's personal. And that may be the questions we should be looking at rather than whether it's personal or not accept to distinguish between commercial businesses and so forth.

So I throw that out. Peter, do you want to follow up on that?

Peter Kimpian: No, no, not necessarily, no. I don't know. No.

Chuck Gomes: Okay. Stephanie.

Stephanie Perrin: Stephanie Perrin for the record. I think that that's a really useful distinction, Chuck. It's my observation that it's very convenient to say something is not personal data. But it is a gray area these days more than ever. And it's much more useful to not panic about whether something is personal data but to discuss what your - what your accountability and your responsibility is to disclose and to disclose or use.

And I think that's where we should be heading and quit panicking about - we can argue until the cows come home over whether something is personal data or not, and it will vary by jurisdiction and by carve-out. We should never have said that business card data was not personal information for the purposes of that act. But that was the political carve-out that happened at the last minute in our jurisdiction. You will find similar really odd carve-outs all around the world. That doesn't help us at ICANN. We should be building privacy by design as Theo said. Thanks.

Chuck Gomes: Thanks, Stephanie. This is Chuck. Susan, go ahead. And we are - notice that we are just about done for the day with our time limit so I'll bring it to a close in a moment. But go ahead, Susan.

Susan Kawaguchi: So I just - quick comment - Susan Kawaguchi for the record. I just think we also need to balance the value of having this information displayed and the purposes and the use. This - the thin Whois data is extremely valuable to me managing a corporate registration. And so I think that, you know, and it's also valuable in my opinion, for an individual, you know, if all of a sudden there's an update or the domain name, you know, that you didn't do, the

registrar or registry, or someone hacked in and to the registrar and made a change to your registration, that's your first clue.

You know, your creation date is important for a lot of reasons. You want to make sure that data always is consistent and doesn't change unless you have proactively changed it. This doesn't really show all the statuses but if somehow my - if Facebook.com becomes unlocked at the registry that's a huge security threat not only for the domain registration but for 1.8 billion users.

So I just think that we need to balance, you know, any of this data - the harm that could be - that could happen by not having that data to rely on and protecting that data.

Chuck Gomes: This is Chuck again. Thanks, Susan. And we will look at the thin data elements one by one and talk about whether they meet the data protection laws as they apply to different jurisdictions. So don't know if we'll get to that next week or not, but we are out of time for this week.

Now my assessment is that we may not have reached any conclusions on anything today so that we don't need to test those via a poll. But if somebody thinks there is something we should evaluate via a poll in the next few days please speak up and let me know.

The - so we're obviously going to have to continue our agenda that we mapped out because we didn't get through it all this week. We will continue it next week. I hope that everybody - that's on it this week can continue next week. I know that's probably impossible. But we're going to have to continue this discussion next week. And we as a leadership team will take a look at it and see if we can reach some decisions in terms of how best to continue the discussion and begin to make some progress with regard to the specific data elements.

So bear with us. Thanks, Peter and Stephanie for playing a special part in this. I'm sure you will continue to do that as we continue to move forward in our working group. If nothing else, I think we realize even more than ever, the complexities of what we're dealing with. But I think if we're all cooperative we will be able to come up with some recommendations that will be helpful. Any questions or anything else that we should cover that I missed, please let us know right now.

Okay, well thanks, everybody. I will adjourn - this is Chuck again - I will adjourn the meeting now and the recording can stop. Have a good rest of the week.

END