UNKNOWN SPEAKER: We will now officially start the recording and the interpretation of this webinar. Good morning, good afternoon, and good evening everyone. Welcome to the at-large capacity building program 2018, and the second webinar on the topic of compliance of the WHOIS registration data with GDPR interim model. We will not be doing the roll call as this is a webinar. If I could please remind all participants on the phone bridge as well as on their computers to mute the speakers and microphones when not speaking. Please don't forget to state your name before speaking, not only for the transcript purposes but to allow our interpreters to identify you on the other language channel. We have English, Spanish, and French interpretation. All lines will be muted during the presentation and unmuted again when we have the question and the answer session. Thank you all for joining and now turning it over to Tijani, chair of the at-large capacity building working group. Thank you very much and over to you Tijani.

TIJANI BEN JAMAA: Thank you Andrea. Good morning, good afternoon, good evening everyone. This is our second webinar for 2018. [inaudible] will be about the company of the WHOIS registrant data with the GDPR, and we will speak more specifically about the interim model put forward by ICANN and all the other [inaudible] from article 29 and also from the accreditation model from the APC and BC. So, we have two presenters, [inaudible] from ACO, and Alan Greenberg, chair of ALAC. I don't know if you have other housekeeping to do Andrea, because we are on a new system. If you have so, please go ahead.

ANDREA: Thank you so much Tijani. As we are using Webex for this webinar, we will not be doing the survey at the end of the meeting. We will, however, email the survey link to all of the participants, so please do take the time to complete this. Your feedback is very important to us. You may continue.

TIJANI BEN JAMAA: Thank you very much Andrea. As I told you, we will have two presenters, the first one will be Thomas Rickert and then Alan Greenberg. I will give the floor to Thomas first and then we'll come back to Alan. Thomas please.

THOMAS RICKERT: Thank you very much Tijani, and hello everyone, good morning, good afternoon, good evening. As Tijani mentioned, my name is Thomas Rickert and I'm working with ACO alternate industry [inaudible] based in Germany with more than 1000 members from more than 70 countries. It is quite international, and we have more than 150 members working in the domain industry and this is why we take a great interest in ICANN development and we have been quite focal when it came to GDPR compliance and the domain industry. Thanks for having me again at this second webinar. I will try to give you an update on where we are with this at the moment, I will also add some explanations, and I should say that as with many legal matters, you can always have different opinions. There's this famous saying, if you have two lawyers you might end up three different opinions. I should just preface this by saying that the

legal opinions that I'm conveying to you are mine or those of ACO and co-authors, of, for example, the GDPR domain industry playbook that we drafted and submitted as a proposal, but there might be other views on those subjects. I have a lot of background noise, so I would like to remind you to mute your mics, unless you have done so. Let's now proceed and dive right into substance, we have two presentations and I will speak probably for roughly 30 minutes, and then we can have some questions on my introductions... introductory talks and then Alan Greenberg will speak and then I guess at the end we will again have some more time for discussions. I am not trying to move slides, there it is. Great. Let's start with a little recap.

As you know, the decisive date for GDPR kicking in will be the 25th May 2018, and since it is a regulation. It will apply immediately throughout Europe. So, other than, for example, directed which needs to be transposed international law, there is no implementation required at the national level for GDPR to be fully applicable. Now the process inside the ICANN community has started quite a while back and just to get everyone aligned on what has happened so far, I have put together some bullet points together to where we are today. Previously, ICANN has asked the community for input, resulting in the submission of several proposals, one of which is the aforementioned paper that we have drafted that [inaudible] other community driven proposals on how ICANN should respond to the GDPR challenge. ICANN then published a plan which has been presented in Abu Dhabi by [inaudible], that the GDPR subject should be dealt with in two different phases, which don't necessarily have to be worked on subsequently but they can be worked on in parallel. The first of which would be a contractual compliance

phase, and this is basically the phase we are in at the moment. The second phase, and that is what gives ICANN it's legitimacy, is the bottom up multistakeholder process that results in ICANN policy, potentially consensus policy that would be applicable to all contracted parties around the world.

We are now talking about the compliance phase, where ICANN shall in an ideal work, forebear enforcement of its contracts relating to those aspects of the contractual relationship with registries and registrars, that have an impact on dealing with personally identifiable data. Because, as you know, if contracted parties make changes to WHOIS or other processes involving PII as we call it, then that would technically be a violation of ICANN contract. The contracted parties are in the predicament of following GDPR and potentially violating ICANN contract, or following ICANN contract [inaudible] and being in violation of the GDPR. That's what the contractual compliance phase is for. Now, ICANN has also hired a law firm, the Hammerson Law Firm, to write memos to my knowledge, there have been 3 memo's that they have published. ICANN has called this peeling the onion, so they have planned to send the Swedish lawyers questions for them to respond and then a second and a third set of questions that should be responded to. That process, to my knowledge, has stopped. We can only speculate about the reasons for Hammerson not having been hired further, but I think we can't expect any further memo's and advice to come from them. Then ICANN published 4 different models, and they said that there were 3 models, but in fact, we had 2 variations of so called model 2, that's 2A and 2B. We went through those models briefly at the end of the first webinar, so not going to explain them during this session.

Those who are interested in those models can either go to the recording transcript of the previous webinar, or to ICANNs website and read through this document outlining the proposals. But, I should also say that these models that ICANN has proposed are of historic value at best, because, we are further down the road now so ICANN has solicited feedback on these models and subsequently come up with a new model, which has been tagged [inaudible] model. The calzone model has been proposed by ICANN after consultations with external stakeholders, such as the article 29 working party, or to be more precise, with a technical sub committee of the article 29 working party. For those, who have either not heard it or forgotten about it, the article 29 group is a group that consists of all European data protection officers, but it is not a formal institute or if you wish, or ministry, or what you have you, within the European Commission. It is an informal group more or less, that can issue advice, but it is not the equivalent of the European Commission, nor can it represent the European Commission. Therefore, you will have seen that there is parallel correspondence going on between ICANN and the article 29 group, and ICANN and the European Commission.

Basically, on the... based on community feedback that ICANN received based on feedback that they got from the GAC, from the European Commission, from the article 29 group and many others who have a concern about ICANN's compliance with GDPR and more importantly about changes to the existing WHOIS system, they came up with something called the calzone model, and the calzone term that some of you might ask, where does that come from. It actually originated from a webinar where [inaudible] said that GDPR compliance discussion more

or less like doing pizza, so everyone has their own ideas, flavors, and ingredients they want on their pizza, therefore all the models look differently, and you have to pick and choose individual ingredients. I couldn't resist asking informally and that is really a tongue in cheek comment that it is interesting that ICANN chose the name calzone because those of you who are into pizza know that calzone is the folded pizza that is the least transparent in terms of ingredient, because you can't see what's in it. The calzone/cookbook model as prepared by ICANN has then been submitted to the article 29 working party for their advice, so ICANN's hope was that the article 29 group would get back with substantive responses and potentially tell ICANN and it's community what can and can't be done, with respect to, in particular, if we're going to talk about details on that as we move on. I should also say that in addition to asking article 29 for feedback to the calzone model, ICANN has also asked for a [inaudible] to allow for ICANN and the community and the contracted parties to have more time to come up with a common solution and to implement it at the technical, operational, and legal level. That was the ultimate goal of avoiding fragmentation in the marketplace, because, if you don't have a unique approach, then everyone will do his or her own thing. During this presentation, I will focus on four points. I will show you through the key components of this draft interim model/calzone/cookbook. We will then look at the article 29 work party response that ICANN received. We will then talk about real and potential consequences of the situation we are in at the moment.

Then I will try to draw some conclusions which will hopefully stimulate a little of discussion with this group. Now, the key elements I haven't

made up but actually have taken those from slide that have been used by ICANN, [inaudible] in particular to inform the community at ICANN 61. So, basically what ICANN is suggesting is that all the data as currently collected by registries and registrars, will enforce the collected. The registrars will collect registrants data, they will collect [inaudible] data, and also the data as required under the data retention specification which is in the appendix, or in the annex to the registrar accreditation agreement in the 2013 version. So, [inaudible] shall be collected. All this data shall be transferred from the registrant to the registrar and it should also be transferred from the registrar to the registry, and this is actually a point that also needs some discussion at least at the legal level, and in fact both points need some discussion, because the GDPR as you will recollect has one of its main pillars which is principal of data minimization. One can argue whether it is actually... whether registrars needs all these contact infos. We do know that registries that collect less, particularly in the ccTLD world and still those registrations work. Do you need [inaudible] data? Or, don't you need that at the registrar level, is the first question that needs debate and ICANN suggested that [inaudible] data needs to be collected.

As far as the transfer of data from the registrar to the registry, we do know, and all of us know, that Verifone can do pretty much without knowing who the registrant for an individual domain name is. They use the same model as we call it. Yet, there are multiple reasons why it can be legally justifiable to transfer all data, including the registrants data to the registry. This is particularly true in an area as well, the registry wants to conduct their own security checks, whether they want to, for example, use the data to validate eligibility requirements they might

have. They might want to detect patterns of illegal behavior, or abusive behavior in that zone. They also might want to wish to be helped to keep a record of who owns what domain name, in order to be able to contribute with all these domain name disputes. This is one of the points where I think it's OK for the registry to know who the registrant is, whether they need all the additional data [inaudible], I think is OK for ICANN to propose, but it is actually a matter that needs some further legal justification. On data retention, you may or may not know that registrars are required to collect and store more data than registration data only. They're required under the aforementioned data retention specification to collect data elements such as the IP address of the registrant that has been used when registering the domain name, payment data, but also information on additional services they have booked. This ICANN requirement is a little bit unclear for my taste, because, it only speaks about data retention but it does not specify whether each registration data only, or whether this also includes the data under the data retention specification, because that is something that doesn't have to be as clear at the moment, we will talk about that [inaudible] in a moment, but we need to discuss what retention period is actually OK for this. ICANN has suggested 2 years and explained this is inline with European data protection laws. I will speak to that a little bit more when we get to the article 29 response. ICANN proposes [inaudible] registration plus 2 years, and ICANN also works on a way that has been granted for shorter retention periods under the so called data retention [inaudible] request program for registrars.

I think I should now talk about... I should add, because I have been conflating the topics a little bit, the [inaudible] subject because in fact it

is the data that needs to be collected under the data retention specification that doesn't have to be as [inaudible].

So, ICANN hasn't specified whether only registrants data, or whether all data including the data retention specification data shall be as [inaudible]. As far as being unclear, like 2 or 3 minutes ago on this point. On the takeability, ICANN has suggested that the model needs to be used for all those that are under the scope of GDPR, that will be processed within the EU, and a little more in the EEA, the European Economic Area. This would include Norway for example. They also said that it can be used at the global level, and that is a suggestion to facilitate doing business for registrars that are operating at the global level, because if this criteria wouldn't have been proposed, then potentially registrars and registries would need to offer and many WHOIS systems, and different processing of personal data as we have jurisdictions in the world that have data protection laws. This allows for a globally applicable system, which makes life easy, I guess, for everyone at the operational and technical level. Then ICANN has suggested that registrations of national, natural, and legal persons can be treated the same. That means that ICANN doesn't force contracted parties to make a distinction between legal and natural persons. That has been a point of huge debate within the community and abroad, because there are legal systems in fact, where the name of companies, even if they have, for example, the founders name in it, which would be a personal data. That such data would not be protected by law. This is something that is difficult to understand, at an international environment. But, GDPR specifies that yes, data's natural purposed will be protected, names of legal entities or of corporations, not necessarily,

but where the company name includes personal data, for example, the name of the founder, that would make it PII. Therefore, it is quite a risk to, for example, publish the names of corporations because you might publicize personal data by doing that.

From registries make that distinction based on the first identification of the registrant. ICANN doesn't force the contracted party to do so, and in my view that is the right way to do this, unless for example, the article 29 will give its blessing to doing that distinction based on first identification of the registrants, which so far they haven't. This has produced risks for contracted parties.

What data shall be publicised in public WHOIS? We have the registrants name and that would not be published. ICANN however, wants the registrant organization to be published, and that is a point of concern because we do know from another... some bigger contracted parties, that more than 60% of all cases, the organization data, or the data in the organization field equals the data in the registrant field. So, if we have concerns publicizing the registrant field, because it might be PII, then the same concerns should apply in considering the publication of the organization field, which I think should not be done. Then registrant postal address shall not be published, only the state, province, and country shall be publicized because that wouldn't allow for the identification of an individual. Registrant [inaudible] that I will subscribe to, registrant email address shall not be publicized but either an anonymized email address or a webform shall be publicized to allow for contactability with registrants, without giving too much of a spoil I can say that from a angle welcomes this criterium. I should add that this is a major step ahead and in fact, I have very much supported anonymized

email address or webform, as it is very less invasive than publicizing an email address of the registrant. However, there are concerns that these, and particularly with anonymized email address. Because, the anonymized email address, if it allows for all emails to be relayed to the real email address, it would allow for spamming the registrant, and also if the registrant is using, for example, an autoresponder, away from mail or to respond, that might lead to undesired publication or response including the real email address of the registrant. Webform should be the preferred method, as [inaudible] uni direction only. Nonetheless, permissions with that potentially as well. Registrant phone and fax number will not be publicized, then for [inaudible] only webform anonymized email address, same thinking as previously mentioned would apply. Phone number for admin and tech would not be publicized, but registrants shall offer an opt out to have WHOIS information published. Let's be clear, if ICANN speaks of an opt in for publicized email address, that would legally constitute the provision of content, and that is not as programmatic as consent can be withdrawn at any time, without giving any reason by the data subject concerned. But having an optional, I think is an OK way forward. Then, when it come to getting access to non public WHOIS data, there were some discussion about, at least for the interim, allowing for self certification of WHOIS customers, and the idea was that the system used for zone file access would be deployed. For those of you who know how zone file access in the ICANN world works, there is hardly any possibility for a registry to deny zone file access, so that would basically open the floodgates for pretty much everyone. ICANN has understood this and will not allow for self certification, even in the interim as long as no accreditation program is set up.

Then when it comes to the accreditation program, which is also used in connection with the term gated access, ie, you have certain data elements that I outlined a moment ago that will be publicized and then you have other data elements that would not be published, but the idea is to allow access to non public WHOIS data elements for those who get certified under an accreditation program. They would then be able to access such data and the idea is to talk to governments and ask the governments to provide lists for law enforcement authorities that shall have access to that data.

The GAC has been asked to develop a code of conduct for law enforcement and other to inform the accreditation program about who shall have access. This has caused some debate at ICANN 61 and the GAC has clarified in the communicate that has subsequently been published that they don't want to be in an operational role with this. Nonetheless member states of GAC members are certainly free to contribute to that process. The GAC has also offered to work on codes of conduct and otherwise help with coming up with a gated access/accreditation system.

I think I am going to skip this one slide, let's now talk briefly about the article 29 response. Basically what they have said, there welcome layered access, said it's a good idea. They also welcome the idea that registrants can be contacted by anonymized email or webform, or other technical need, so that's good. Then the issues start, because they say that the list of purposes that ICANN outlined, such as, [inaudible] stability, IP interest, law enforcement. That this big menu of purposes that ICANN proposed to be lawful purposes to allow for access to non public data is too broad. They reminded ICANN of the principle of

purpose limitation, and that all purposes need to be linked to a legal ground, which in the current document hasn't taken place. Also, they asked ICANN to ensure that no purpose is pursued by other interests, by third party interests. These interests should not determine the purpose of pursuit by ICANN. Third party interests and ICANN's own interest should not be conflated. They also take note of ICANN's intention to undertake legal analysis with respect to gated access and stuff like that. In my view, this language translates to it is not there yet. ICANN has not offered sufficient detail, or sufficient legal analysis, legal rationale, to even allow for the article 29 group to assess whether ICANN's proposals are good or bad as it is lacking detail. Then they've clarified that there shouldn't be any bulk access, just individual requests for individual domain names. So the ideas voiced by the GAC and others that there should be unlimited access to non public WHOIS data that there should be the possibility to do reverse lookups, that there should be the possibility of non traceable WHOIS requests. I guess that will not happen, because the article 29 group is looking for limitation and safeguards so that not all WHOIS data, not all non public data can be mined.

Then they say that there should be binding contractual agreements, which so far hasn't been proposed between the registries, the registrars, and ICANN on the respective roles. I am going to speak to that in a moment, towards the end of my introduction. Then they also speak to the issue of data retention and they say that ICANN didn't offer any robust rationale for picking exactly life of registration plus 2 years, and that this is not good enough reason to retain data for that long. In fact, when ICANN mentioned in the [inaudible] that the 2 years are in

line with European data protection laws, at least [inaudible] been able to identify any such law in Europe that would require such 2 year retention period. More work needs to be done on that.

What are the consequences of that? ICANN has obviously failed to trigger a response from the article 29 working party, the hope that the article 29 working party would fill the blanks in the cookbook has been disappointed. So, we find ourselves in a situation now where there is no detailed guidance on what can be and can't be done. There is just some guidance on what further works needs to be done, but little advice on concrete return. The contracted parties are now forced to implement solutions that they think help them to be compliant, because at the moment we don't have any binding or any agreed upon ICANN interim solutions. There is certainly the possibility for ICANN to come up with emergency policies and probably can talk about that later during this webinar. The consequence of that will be, solutions will not be uniform, and you can call that fragmentation. We see that in the ccTLD work, at the moment already, where all the CC's that are not governed by central organizations such as ICANN come up with their own proposals to respond to the GDPR challenges. Another consequence is that in the absence of a proposal that has been blessed by article 29 on accreditation of WHOIS customers, we don't have a central accreditation body, nor do we have any criteria that has been agreed upon for accreditation. The parameters for accreditation are widely unknown and for full disclosure, even if we had received them last week, there wouldn't have been any change to operationalize a global accreditation system, as that is too big of an undertaking. Then you should expect that WHOIS request for disclosure of non public WHOIS

data will be dealt with more or less manually by the contracted parties and the accreditation model will certainly not make all the WHOIS customers happy, as there is some who would hope that there is an easy solution to this, that there is a one size fits all solution, more or less, to this, and the article 29 group has reminded ICANN that the response to all this needs to be very long.

My conclusions are, and in fact, these are... this is my personal opinion, so if you don't like it, pin it on me. I think ICANN needs to sit together with the contracted parties to start with. Even before wider community debate can take place, to talk about roles and responsibilities. Come May 25th, according to GDPR, data subjects and even registrants needs to be informed in the privacy policy about the roles and responsibilities of the parties involved. So far, ICANN has not even acknowledged that they are a joint controller, they said they might be that, and stuff like that, but to do thing right you would need to have a joint controller agreement between registries, registrars, and ICANN, and that discussion has not started.

So, the contracted parties and ICANN should sit together and talk about who does what. That's not only with respect to registering domain names, but also with respect to who is the controller and processor for the [inaudible] or for the [inaudible] agent, and all these different scenarios that we find. The article 29 group will certainly not do that job, I think they've made that abundantly clear. I think they will at best, comment on very concrete and detailed proposals coming from ICANN. I should also say that we have a lot of detail out there on what can and can't be done. The playbook that I have co-authored that is published on ICANN's website has a community proposal, has a lot of such detail

but it hasn't to a huge extent, not made its way to the cookbook. I am going to skip this, but this is just all the parties involved in the iCANN eco-system. So, we also need to talk about the collection part. Do we really need a billing [inaudible]. I am not aware of any registrar who looks up the WHOIS data for the billing contact to send invoices. What they do is they send invoices to the account holder. We need to look at all the questions surrounding collection and that discussion hasn't really started. Controller process, I have discussed a moment ago. Then we need to discuss more what the parameters for an accreditation system should be. At the moment, and that is my observation, many players do not say that WHOIS is so important and that the world is going to stop revolving if public WHOIS stops, for all sorts of reasons and all those reasons I can't understand, from consumer protection to brand protection, to child protection, to what have you. That's all good and fine, but you really need to dive in to this and look at the legal justification, the purpose and international transfers in order to make this happen. We need a discussion that is driven by legal parameters and not by emotional arguments and by particular interests.

Let's move to [inaudible], which is my last slide. We need to discuss and I'm just going to give you some buzz words, when it comes to allowing access to WHOIS data or responding to the affirmative to disclosure requests, we need to make a distinction between different customer [inaudible], IP interests, security researchers, consumer protection agencies, domain traders, who also want to get access to that data. When it comes to LEA, law enforcement authorities, who are just talking about law enforcement, but actually we need to be far new nuance, we need to... there are different legal implications in all these five scenarios

that I've outlined. Just to stick to my homeland, if a German law enforcement authority talks to German registrar, that's different from French law enforcement asking a German registrar, that is yet different from a US law enforcement asking a European registrar or registry. That is yet different from the FBI asking the US contracted party to disclose data, and it's yet different from a third country law enforcement asking a US or a Canadian contracted party for disclosure of data, right. This level of detail, I think we have something in the draw for that, but I think ICANN has yet proposed details on this in their communications to the community and the article 29 group. We do need to do that, and we also need to answer questions such as, who needs access to what. What data elements do people actually need. Security researchers, they want all the data. I guess they can't have it, but who can think about offering them [inaudible] which also allows for them to identify patterns of illegal behavior.

I guess that we should sit down, do more work, and then get back to the article 29 group with substantial, where the [inaudible] proposal, with a lot more detail, together with the contracted parties to start with, and then we need to advance the community process as you may know the RDS PDP working group has been paused, but we're hoping for the work to be resumed as soon as we can in, probably in a different format. I will conclude with this, we need to continue to advocate for ICANN's important mission and role, and that includes the multistakeholder model as we're seeing first tendencies that in the light of GDPR, in the light of the WHOIS resort not being as available as today in the months to come, that people are questioning ICANN's authority and questioning whether ICANN is better placed to be regulated. I think this would be a

disastrous side effect of this debate, I think we can be compliant and yet do things that are possible in other industry as well. This [inaudible] doing their jobs properly. I think, I should stop here. Thank you for your patience with me, for your interest. I'm not sure Tijani whether we want to take some questions now or move to Alan.

TIJANI BEN JAMAA: Thank you very much Thomas for this presentation. [inaudible] even if you gave your point of view, it's also nice [inaudible] explain to our community the interim model, and to give them information about all the inputs we've received so far. It was very good done, thank you very much. [inaudible] our own condition [inaudible]. Now there is 2 options, we may take some questions for you if there is, if there are. If there are not, we can go immediately to Alan. Is there questions for Thomas?

ANGELA: I do see that Olivier has his hand up.

TIJANI BEN JAMAA: Olivier please go ahead.

OLIVIER CREPIN-LEBOND: Thank you very much Tijani. Olivier Crepin-Lebond speaking, can you hear me?

TIJANI BEN JAMAA: Very well.

OLIVIER CREPIN-LEBOND: Thank you. Thanks very much for the presentation Thomas, really interesting as always and great to have you go into details on this, really important topic. I have a question when it comes on to the WHOIS service in itself. We've read in the press that WHOIS is effectively dead as it is currently running, or at least it has been alleged that it is currently dead and yet at the ICANN meeting in Puerto Rico, we had the [inaudible] the new guy in NCIA, the new head of NCIA. [inaudible] replacement saying that the United States is committed to having WHOIS which has full details of registrars, at least that's sort of paraphrasing of what he said. Where did we sit on this? And how is ICANN going to be able to satisfy both sides?

THOMAS RICKERT: I think this is going to be a major challenge to be quite honest, and will seem, I guess from escalation of this in previous one, in recent communications, we have completely opposite concepts in the US versus Europe on data protection. I guess, there's no way for the European commission to easily say we're going to honor the wish of Mr [inaudible] and just keep data published. However, that doesn't mean that there are no ways for hurdles to be overcome. In my view if a US entity, for example, is approached by a US law enforcement authority that is, that has jurisdiction over the registrar. The registrars in the US certainly needs to follow orders and disclosure requests from local law enforcement according to [inaudible] national laws. Even those such disclosure might not be in line with GDPR if somebody contacts with an entity in the US, it is not entirely surprising that the US entity is required

to follow its local laws and be compliant over there. I guess that, if you go to the different scenarios that I've outlined, there will be possibilities. Also, I should note that there are ccTLD operators, who have not offered a public WHOIS service for many years. To give you an example, [inaudible] operating the dot FR domain name, receives something in the order in the magnitude of 300 disclosure requests per year. I think this might be manageable, I think we need to be smart about processes to help with potentially synonymized data instead of real registrant data, and also it is possible for governments to come up with legal instrument to get access to data more easily. In Europe for example, there is the police director, which can authorize certain processing activities and that can equip both public as well as private entities with certain rights, yet the European lawmakers have not yet [inaudible] themselves of the opportunity of doing this. Or lawmakers could establish a legal requirement whereby certain data needs to be publicized. The analogy to trademark patent and patent databases and design data bases, or commercial registers are often made, and people are asking why can we publish data there and not in the WHOIS, that is a contradiction. The difference is that for all of these public registers, there is a legal basis for publicizing the data. I think as we move on, there will be solutions emerging. I think if we specify who needs to get data on what legal basis and for what purpose, you will see clear on what the possibilities and what the limitations are, I can promise not everyone will be happy, but I think that probably more can be done than currently meets the eye, because all this talk about WHOIS is going to go entirely dark, I think that's not going to happen. I think law enforcement will still be able to do their job. It might be a little bit more cumbersome, but I think there will be solutions.

TIJANI BEN JAMAA: Thank you Thomas. Thomas, what you said is absolutely true. I think that there will be solutions, despite the disappointing response of article 29. Article 29 working party [inaudible] this is I think a [inaudible] they don't have the [inaudible], but this is... they are... their opinion on their recommendation is very slow to what the European jurisdiction or European know, the European regulation says. I think that we can do better if we have a good response from article 29. Now we have a meeting planned in Brussels in upcoming days and I hope that there will be a good result. Any other questions? Andrea are there any other hands, I don't see hands?

ANDREA: It looks like Olivier's hand is up again. Olivier.

OLIVIER CREPIN-LEBOND: Thanks very much. Olivier Crepin-Lebond speaking. I have many questions but I do want other people to ask questions as well. That is why I put my hand down. If nobody else wants to ask questions... the next question that I have is with regards to ICANN itself and to contracted parties. It was hoped that whilst the plans were being made in Puerto Rico, that showing that ICANN and all parties involved are actually working on this quite hard and proposing solutions, would effectively soften the stance of the article 29 of the commission, with regards to ICANN and say, well you know you guys are working a solution out, so we're going to give you an additional amount of time, or at least we're not going to bring enforcement on your shoulders right

now. From what I've heard, from what you've said Thomas. You've said that an actual reprieve or a moratorium that ICANN did ask in it's listing, in it's proposal, that was refused. Does this actually mean that ICANN and contracted parties, where the registries and registrars operating in Europe are open to get prosecuted from the day after enforcement comes into effect? Or, does it not point to that direction? Is there still likely to be some flexibility here? Or does one not know.

THOMAS RICKERT: Thanks for the question Olivier. The article 29 group has simply ignored that request, and I think that can translated to a no, no moratorium. I've asked myself what the legal basis for a moratorium or what the authority should be for the article 29 group to grant a moratorium, I think that it is OK for ICANN to try, but I didn't have any hope that the article 29 group could possibly offer such moratorium. On top of that, the European Commission alert has continuously emphasized the dependence of the individual data protection authorities, so you can't easily put a spell on independent authorities and tell them not to do what their legal mandate is, ie, to take action on complaints coming from the public. I think they will potentially take action against contracted parties, but the question is, will this be a priority for the DCA for proactive action, and my take on this is, and I have no reason to prove this, I think that given the complexity of all this, given the requests from law enforcement to give it... to keep the system as open as possible. Not only non European law enforcement, but also European law enforcement. There should be sympathy for the contracted parties and ICANN to sort of try what they can, that they push it back and not jump to conclusions prematurely, to find solutions to maintain the

status quo as much as possible. I think they will likely not be inclined to sanction proactively, but if there are consumer complaints about registries or registrars wrongly handling their data, the authorities will need to take action as under GDPR they can be sued for inaction as well, so they need to react then, but if they can show that they have done what they could in order to start the process of becoming compliant, I think that will have an impact on at least the amount of fines that might be in question.

TIJANI BEN JAMAA: Thank you Thomas. If there is not other people asking questions, Olivier you will speak to the other questions at the end so that you will have Alan's presentation and we will answer all the questions at the end. Can you do that? Alan are you ready?

ALAN GREENBERG: I'm here.

TIJANI BEN JAMAA: OK, please go ahead.

ALAN GREENBERG: Thank you very much, just let me get the slides so I can see them. Next slide please. Alright, first of all, thank you to Thomas who outlined an awful lot of the details and the pros and cons. Thomas touched into this, but I want to make sure that everyone understands as it's an interesting situation. Normally we have policy setting rules, the contractual

compliance model essentially says we're going to ignore some rules, the rules that require you to publish certain data. That's one technique that can be used, if the legality of it is not clear, and it's not clear that all of the things that we're asking registrars to do are purely negatives, that is not enforcement things. There's another tact that board could take, the board can set interim policy, so they tomorrow could essentially create a policy replacing the current WHOIS rules, and that policy can have effect for 1 year. It would be up to the GNSO to create a formal policy to replace it in that period of time, given what we know about GNSO PDPs, doing something with 1 year is an interesting challenge, but in fact that is something that the GNSO has been presented with, that it may well happen quickly and they may have to do this and there... in fact, if that comes to be, there's a session being scheduled at ICANN 62 that may look at that. We have a number of interesting tasks going forward. Next slide please.

Andrea, next slide please. As Thomas has laid out, this model has problems. The reasons for collecting data have not been well presented, but that doesn't mean that they are not justifiable and can't be done. The process going forward has to be to look at... we have no choice but to be GDPR compliant, but the interpretation is going to be interesting as we go forward. Tools to have selective access to data is a key, and it's one that we should have started working on very long time ago, and Thomas mentioned this also, the accreditation model is not going to happen quickly and I have no comprehension why ICANN has delayed even thinking about it until now, when it has been known for a very long time that it's one of the key aspects that will be required. Next slide please. Part of what I'm doing here is looking at the negatives of the

model that has been proposed and how it is being handled. It's clear that the model goes further than is necessary under GDPR. GDPR requires that information about natural persons, people, be protected but not legal persons, companies. Our model that has been presented by ICANN says I'll treat them all the same. GDPR requires certain treatment of, within residents within certain territories, we have said registrars can go ahead and do everything. Now, this is not just problematic philosophically, it's also counter to the GAC advice and I think most of us understand that if ICANN is going to go forward with something counter to GAC advice, we have a serious issue that is going to have to be addressed.

Another example is of ICANN looking for simple techniques which I don't think are ultimately going to work, is the proposal for anonymized email address. First of all, it's a problematic proposal in that if you go back to the original causes, of reasons for having WHOIS, and some people like to talk about the original one. It was to be able to fix the network. Anonymized email address is very difficult to address that. If your mail doesn't get a response, doesn't mean that the address that they gave no longer work, doesn't mean they are simply ignoring you, you don't get an answer back saying, oh well the email company works, but the user doesn't exist, or the whole address is bogus. You don't get nearly as much information, but as important, anonymized email says we don't give you the real address, we give you an anonymized one, but the way its been discussed, every time you register a name with your same email address, you'll get a new anonymized address. A lot of the pattern matching, that is one of the keys for fighting cyber abuse, spam, and phishing, is the ability to recognize this has been registered by the

same name, by the same entity, via the email address, and that goes. Next slide please.

One of the keys that the article 29 letter... we went two slides, one back. No, one forward. OK, hold on. Let me figure out what's the right number. It was on the screen for a second then disappeared.

ANGELA: This is slide 5 it says [inaudible].

ALAN GREENBERG: Hold on. I'll tell you which number we're looking for. OK, sorry we are on 6. You skipped to 7 and I thought that was the next one.

ANGELA: OK, great. Thank you.

ALAN GREENBERG: OK. Now, one of the questions is why do I care? I'm the chair of ALAC, and we say we care about users and there's a lot more users than registrants, so although privacy is important, why does it matter to the 4 billion users? Why is matters, one of the key reasons, is WHOIS is a major tool used in combating cyber abuse. It helps combat phishing, spam, and spam is not only annoying, spam is the major vehicle for malware distribution. Domain name abuse, and I'll talk about that in a little bit. It really is a major issue for at-large. Let's go onto the next slide please.

Now, one of the key statements I found in the article 29 letter, is this statement and I'll let you take a moment to read it. It basically is saying that ICANN should stay out of other people's business, worry about what data they need and don't worry about other things. Next slide. Here's ICANN's mission, right out of the bylaws. The mission of an internet corporation for assigned names and numbers is to ensure the stable secure operation to unique identifiers. Now implicit in operating the DNS is operating it, so that it is trusted. If you cannot trust that when you enter a URL that it gets to the right place, then the DNS has no value whatsoever. That's one of the reasons why we put DNSSEC in place, because that helps ensure that no one can corrupt the DNS and provide information which will to get you to the wrong place, when you think you're going to another place. Next slide. As you look, this is a repeat of the previous slide, it is not an accident, so they are saying that we should not worry about how other people can get data to do their job and for the lawful processing, now next slide. Some of you may know what the term catch-22 is, it's an expression that comes from a book that's written about 60 years ago, that describes a situation where you have two situations which are opposite and cannot co-exist, it makes no sense for them to co-exist, and that's exactly the situation we have in the current implementation of GDPR and WHOIS information. If we ignore the uses that law enforcement, cyber abuse fighters, and people like that... rather if we ignore their uses, and we cannot collect the data, because collecting is use is, is processing of the data. If it isn't collected, it can't be used no matter what the need. ICANN is the only body that can set the rules for what is collected, and if we don't specify that this data has to be collected, then it cannot be made available to law enforcement, cyber abuse, or anyone else. Implicit in our building a

trusted DNS, we must be able to provide the tools and the data to the other parties around the world to help ensure that it is a trusted entity. We cannot give away that responsibility, if we give it away there's no one else to take it. There is no one else to force the registrars to collect the data and store the data so that it can be used. Next slide.

Now, what next. As Thomas or Olivier mentioned, someone, we've made a request to delay. As far as I understand, and Thomas alluded to that at the end, I don't believe the data commissioners have the jurisdiction to grant a delay. So, clearly they cannot grant a delay, there are other mechanisms in which a delay could be granted, but certainly it is not the data commissioners as far as I understand. We are likely to see a lot of almost random implementations, from complete blackout of WHOIS to something that might be a lot less. To a large extent, we may see a functional black out of WHOIS. Olivier mentioned the US government and that is one of the other interesting unknowns. The US as a believer in a free WHOIS, has said clearly US companies have to be compliant with GDPR to the extent that they have European customers or at present [inaudible]. Except in those cases they believe all the WHOIS data should still be made available. They could pass legislation requiring that data to be made available where it is not countered to GDPR. I don't... I'm not predicting that will happen. It is an interesting situation and how registrars would react to it might be interesting, but it's certainly one of the things that we have to look going forward that just could be happening as we move. Next slide please.

What are some of the implications? Well, the GAC has given advice saying they want WHOIS to be as open as possible, and that of course is driven by the fact that the GAC has tended to be closer to their law

enforcement counterparts within their own governments than their privacy offices. So, we have a GAC subgroup looking at cyber crime issues, we don't have one looking at privacy issues. The GAC has come out very strongly saying that it is important not to shut down WHOIS. We've already mentioned the US is... has a quite strong position on that and we don't know how that's going to come on show as we get closer to May 25th. Anyone who owns a domain name has the right under ICANN policy to transfer that domain name to another registrar, that can't be done if WHOIS information isn't available. There are an awful lot of people who register domain names, trying to capitalize on trade names. If you type in right now Anazon, that is you type in N instead of an M for Amazon, or Facebock, which looks an awful lot like Facebook, you'll get to the right site, and you'll get to the right site because these are domain names that have been registered and through the process that ICANN developed to allow a domain holder and intellectual property holder, or trademark holder to get that name back. Those names now point to the right site, but when they pointed to the wrong site, they were tracking hundreds of thousands of clicks per day that often went to things like phishing sites, trying to get peoples credentials. Everyone who uses email, pretty much everyone depends on spam filters. These spam filters depend on services that use WHOIS. If you go to a site on your web browser and it has been problematic, you will probably get a message flashing up from your web browser saying this site cannot be trusted, do you really want to go there? Those depend on services that use WHOIS.

So, we have an awful lot of things going on in the world, even if individual people don't go to WHOIS, we have an awful lot of things that

depend on WHOIS. Next slide please. I guess that sentence says it all. It's going to be an interesting could of months, it's probably going to be an interesting couple of years. We have a very far way to go to figure out how to be GDPR compliant, and I suspect, I have no ability to affect it, but I suspect that the laws and the interpretation of the laws are going to have to change as I don't think they were quite designed with this issue in mind and the world depends on the internet now, in ways that are non trivial. A huge amount of the worlds commerce depends on the internet and we can't just say well, if it doesn't work as well, or something happens, we don't really care. I think we're going to see an interesting set of things happening over the next months and years, and it's going to be a real challenge to make it all work. Thank you.

TIJANI BEN JAMAA: Thank you very much Alan. It will be really interesting. Now, is there any questions to Alan first? Angela, I don't see any hands, do you see one?

ANGELA: Yes, Olivier. Your hand is up, you may begin.

OLIVIER CREPIN-LEBOND: Thank you very much. Olivier Crepin-Lebond speaking. So, thanks for this and that's really interesting as well and particularly when it comes down to looking at the WHOIS issues from a users perspective. My question in regards to the registration directory services working group, as you know they have been working for goodness how long, and we've had some review teams and also some other parallel processes taking

place. Where is the work of that going bearing in mind what is going on now with GDPR, and with the current process?

ALAN GREENBERG: Well, I'll take the question from Olivier. It's Alan. Currently that group is halted, it is not clear what is going to happen, it could be restarted, it could be shit down altogether, and as I mentioned if the board chooses to enact a policy, that policy... which they can do under the current contracts. That policy has a duration of one year, and although maybe there are games to be played to extend it, I think we would have to take that one year period seriously. This was presented to the GNSO as a possibility in San Juan, and they are discussing if this were to happen, what could they do, how could they react to create a policy to replace the interim policy and do it within a one year period. I suspect if they were to do that, they would do it with a different working group, with a different set of constraints and rules, and as I said, if it looks like we're moving in that direction by the time we get to Panama, then there will be a session that will look for community input on how could this work. It is not clear at all where the RDS PDP is going right now. Right now it's halted and it may restart, it may not.

TIJANI BEN JAMAA: Thank you. Any other questions?

ANGELA: Olivier, did you have another question?

OLIVIER CREPIN-LEBOND: Yes I do, but I hope other people will ask questions.

ALAN GREENBERG: You're the only one with their hand up.

ANGELA: [inaudible] you can raise your hand, if you are on the audio only, you can speak the lines are open.

OLIVIER CREPIN-LEBOND: OK, so it's Olivier Crepin-Lebond speaking again. The next question is to do with the article 29 group and the commission and the GAC. We are hearing on the one hand that the article 29 and the European Commission are setting the GDPR to effectively focus, primarily on privacy issues, and are taking a stance which will effectively knock out much the information that is currently freely available on WHOIS. Yet, when one looks at the GAC itself, it seems that the GAC is looking at entirely the opposite direction and is having issues with regards to law enforcement and therefore wishes to have as much information as possible in the new WHOIS. Is this something that should really be worked out at the end of the day in the GAC? It sounds as though the left hand is doing something and the right hand doesn't agree with what the left hand is doing. These are countries, aren't they?

ALAN GREENBERG: Olivier, it's Alan. Let me give a quick answer and then perhaps Thomas will give you his version of the answer. If you look at the ICANN

correspondence page, there's also a letter from the EU to ICANN saying it's really important to maintain access to WHOIS, not only by law enforcement but to the non law enforcement cyber abuse people. I think the answer is not that it has to be worked out in the GAC. I think the answer has to be worked out in the European Union.

THOMAS RICKERT: This is Thomas. Olivier, it is a great question as it shows a lot of it what dilemma's we are in, at times in dealing with the GAC. I think some of the advice and the information that we're trying to communicate is information based on the experience and the knowledge of the GAC representatives, or the GAC representative maybe in conjunction with critics from other ministries. But what you rarely find is a view that has been formed at the national government level, that has been informed by all relevant ministries and departments. What we see, and I guess it's sort of linked to what Alan mentioned earlier, that we have a group where law enforcement is represented, but we don't have a group where privacy people are present, and therefore sometimes the views that are formed inside the GAC are formed by law enforcement primarily. I guess we've seen that in the past when it came to the RAA 2013 with the data retention requirement, where things have been written up that are clearly not sustainable legally in many jurisdictions in Europe. How can this be solved? I guess, it would help [inaudible] if we could ensure, which by the way we can't, that all governments when chiming into discussions at the GAC level, do this based on what can and what can't be done according to national laws, but here specifically I guess, everyone needs to put their own interests on the record, which is what we see, not only from the public sector but also from other

interest groups, and we need to do something that is compliant in the first. I think there have been some omissions by the lawmakers of Europe to take into account the legitimate interests of law enforcements and others that do need that data, but what we can't do is just basically put pressure on ICANN to do things that jeopardise the contracted parties that trust ICANN. Because ICANN is [inaudible] how data has been dealt with, according to my view and the view of many others, ICANN is at least a joint controllers, and therefore ICANN is also facing the risk of also being sanctioned. We need to fit together with those who are going to enforce, they need to sit together with those who are making the laws, so that they get solutions that help keeping the system as operational as possible, given the current legal situation and help to inform the lawmakers when it comes to a national laws, as well as international laws so that the interest [inaudible] domain name industry and beyond are taken into account.

TIJANI BEN JAMAA: Thank you so much. Any other questions Olivier?

OLIVIER CREPIN-LEBOND: Thank you very much Tijani. Yeah I put my hand up again. Olivier Crepin-Lebond speaking for the transcript and one last question I promise now, as it is getting a bit late here. Earlier Thomas you mentioned about fragmentation, you mentioned that if a solution wasn't found we might risk fragmentation. Yet when I hear about fragmentation, I keep on thinking, fragmentation of the internet is like the internet going into many smaller networks and like with bridges or tunnels or something in

between the networks, or maybe more than one DNS. I've never heard of the term fragmentation when it comes down to WHOIS, could you please elaborate?

THOMAS RICKERT: Sure. I think what the gTLD benefits from, is that we have a central organization at the ICANN, and not only the ICANN organization but the multistakeholder community that sets rules and that allows for [inaudible]. It is not God given that you can transfer a domain name from one registrar to the other. All these things work because there's ICANN setting standards. What we see now is that all the contracted parties didn't get the guidance that they were hoping for from ICANN, nor did they get it from the article 29 group. Now they need to do what they think is best to protect their companies and to ensure compliance. You will see different treatment of WHOIS and other aspects relating to personal data, so some will collect the [inaudible] WHOIS data required by ICANN, others will only collect the subset. Some will not send data to the registries, they will keep the data at the registrar level, or they will just send placeholder data to the registries. There will be different solutions to what can be seen publicly in terms of WHOIS, so there will be some who were not even publicized an anonymized email address or webform as they will think that in itself goes to far and is risky. There is nothing giving them comfort or asking for unity, and we don't have answers from the simplest things. The controller processor question is unresolved, ICANN hasn't started that discussion. So people... registrars need to take a guess what the registry might require what to do, because so far many registries haven't updated their policies and given guidance to the registrars in terms of their requirements, and the

registries don't know what to do because ICANN hasn't told them what to do, right. So, it's a little bit like a daisy chain, where from reseller to registrar to registry, there's a lot of uncertainty. At the moment, there are a lot of registrars who say if the registry doesn't explicitly tell me what data they want and for what reason, and on what legal basis, I am going to send them nothing. That's what I mean by fragmentation, you see the same the in ccTLD world. We see so many different implementations of GDPR, because they are basically on their own. They have their own legal national requirements, and they are trying to do their best to be compliant, I think many of them have been waiting for the gTLD world to set a good example on how things can be done in a uniform fashion, but, this exercise has not worked out. At least for the interIm, we are not going to see anything centralized, if you want to get access to personal data, you will likely be forced to go to the registrar directly and your request will be processed manually based on standards that the registry has set for itself in the absence of global guidance.

TIJANI BEN JAMAA: Thank you so much. In fact, you are absolutely right. If we don't have a model of ICANN [inaudible] before 25th May, of course, anyone will ask as he or she understand they are protecting themselves from any... but I think that there is, in any case, even if we have a good model and it is in place before the 25th May. It will be a kind of fragmentation, because there will be different [inaudible] European registrants or [inaudible] and data of the other people. We don't need to comply with GDPR for the other. It is also kind of fragmentation, two types of treatment, so I think it is interesting situation and I hope that we have better image, I

hope that the meeting with article 29 working party. ICANN can give good solution, or good output, it will help. Perhaps having something better before 25th May. Any other questions?

ANGELA: Yes, we do have a question from a participant on the audio only, [inaudible] you may ask your question.

TIJANI BEN JAMAA: OK. Go ahead.

UNKNOWN SPEAKER: This is [inaudible] speaking, actually I wanted to make a comment rather than a question. The GDPR is actually something that changes on all scenarios. Here we have two legitimate rights that are in opposition. One that is defended by ICANN and the other is the protection of personal data. The personal data protection [inaudible] has basic principles, reasonability, and proportionality of importance, which at the time of the [inaudible] in such conflict situations, we should not be working under so genetic rules. If we consider how the laws operate, I am sure that whenever concrete cases are to be discussed, and I'm certain that there will be many, generic principles cannot be applied. In each case, authorities should see how to implement the reasonability and proportionality principles of each situation. I apologize if this is out of place, but I guess we should also lead the data protection authorities to see how their own principles should be applied. I maybe speaking perhaps too much, but I think this is valid. So, again, here we have two

rights at stake, both are legitimate and in each conflict case, which will all be different because these situations are quite complicated and actually very new, for each case there will be a different solution. I think we should not be so radical here, because their own principles say that, or require specific analysis for each situation, that is the comment I wanted to make. Thank you for this time.

TIJANI BEN JAMAA: Thank you very much. Do you have any comments on her comment? Alan or Thomas? No. OK. Any other questions? Andrea?

ANGELA: At this time there are no other hands on the Webex. Is there anybody on the audio only who would like to speak?

ALAN GREENBERG: Olivier does have his hand up.

THOMAS RICKERT: This is Thomas, before we go to Olivier I wasn't fast enough to offer a quick comment on what we previously heard. I think that balancing of rights is an important thing. Proportionality is an important principle as well, and I think that it's particularly true when it comes to processing data based on the legitimate interest claim to be present with the controller of a third party. That is something that is pretty much in the focus when we discuss accreditation systems. I guess that many of the aspects that we find in the GDPR are quite binary, so some questions we

can look at legal literature, we can look at court decisions and say OK, we have to do this or that with a good chance of being right. With this particular processing based on legitimate interests, you need to do a balancing act, you need to check whether the interests of the controller outweigh the rights of the data subject concerned, and naturally there are contracted parties who are facing liability risks, don't want to take too big risks. In that regard, I think the article 29 group can be a great help by issuing opinions that are in a form of documents that the article 29 group uses often. They can specify whether they think that publicizing data for certain purposes or passing on for certain purposes would actually outwight the interests of the data subject. I guess they can apply those principles that you have so eloquently mentioned and help guide the ICANN community in this process. Thank you.

TIJANI BEN JAMAA: Thank you very much. Olivier. Olivier?

ANGELA: Olivier, you can ask your question.

OLIVIER CREPIN-LEBOND: It took a little more time to unmute. Thank you. Olivier Crepin-Lebond speaking. One more question, we keep on speaking about WHOIS, because obviously these contain the most records, but what about the start of authority records in the DNS itself, which do provide an email address for the... usually technical contact that is related to the DNS record of the actual domain name itself. I haven't seen anywhere it's

been mandatory where this should not be personalized in any way. I know that in general, this detail is given as a sort of generic detail. So, it's like tech@domain.com or dns@domain.com or whatever, but could that be an answer to the question regarding the DNS... well the WHOIS original feelings which was that we need to have a technical contact if something goes wrong?

ALAN GREENBERG: Who are you asking Olivier?

OLIVIER CREPIN-LEBOND: Maybe you Alan, I haven't asked any questions to you yet. Alan?

ANGELA: Alan, are you still connected?

ALAN GREENBERG: Sorry I was talking and I was on mute. Olivier, it's an interesting question and I think it also is linked to the contention I have, that if a legal person chooses to put an email address in their WHOIS record, which for instance has a persons name, so if you as the domain administrator of IBM, have OlivierCrepin-Lebond@IBM.com as the contact, that's an issue that I believe that IBM has to consider in their responsibility in protecting privacy, private information. If you as a legal person, put in information which reveals personal information, where you could have put domain administrator@IBM.com. I think you have done that willingly, and if you violated privacy, it's you that has violated

privacy, not the registrar who is simply passing on that data. I think the same goes for the start of authority records. Whether you put a person's name in or a tech@ is purely your discretion, and you can change that at any time to another address and we know email addresses are readily available in this world, that don't necessarily have personal information. It's the same as if you use a handle on a bulletin board or a game that you play, if you choose to put Olivier Crepin-Lebond as your handle, you are consciously making that decision. You could put the dark avenger instead and it would be just as valid. I think those all fall under the category of, you have consciously decided to do it and I don't see how that can be treated as personal information that was unwillingly put there. Thank you.

TIJANI BEN JAMAA: Thank you very much Alan. We are running out of time now. We have another hand Andrea?

ANDREA: At this time there are no other hands on Webex.

TIJANI BEN JAMAA: OK. Thank you very much. I would like to thank Thomas Rickert and Alan Greenberg for the presentations they did on [inaudible] discussions. I also thank all our participants, and our staff. Thank you very much everyone, and thank you for coming and participating in [inaudible] is now adjourned. Thank you very much.

ALAN GREENBERG: Thank you.

UNKNOWN SPEAKER: Thank you, this concludes today's webinar. Please disconnect all lines and have a wonderful rest of your day.

[END OF TRANSCRIPTION]