**ICANN Transcription**

**GNSO Temp Spec gTLD RD EPDP – Phase 2**

**Thursday 08, August 2019 at 1400 UTC**

Note: Although the transcription is largely accurate, in some cases it is incomplete or inaccurate due to inaudible passages or transcription errors. It is posted as an aid to understanding the proceedings at the meeting, but should not be treated as an authoritative record. The audio is also available at: https://icann.zoom.us/recording/play/e2fELUaDksK_IaRJvsfbsLBvlyF6rg8DSweI4oYLEZeuh3OwI2p8w3G_z_8EaDOA

Zoom Recording: https://icann.zoom.us/recording/play/LHFFiTIs6OzmuuRkAhqqiL5gGGOdkF5LhWtPrwPy3GkVBB-ud-P4LTPX--i63nVz?startTime=1565272820000

Attendance is on the wiki page: https://community.icann.org/x/nKajBg

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

TERRI AGNEW: Good morning, good afternoon, and good evening. Welcome to the GNSO EPDP Phase 2 Team meeting taking place on the 8th of August 2019 at 14:00 UTC.

In the interest of time, there will be no roll call. Attendance will be taken by the Zoom room. If you're only on the telephone, could you please identify yourselves now? Hearing no one, we have listed apologies from Matt Serlin of RrSG. Georgios … it looks like Georgios has joined, actually. Julf Helsingius of NCSG and Alan Deacon of IPC. They have formally assigned Sarah Wyld, Tatiana

Tropina, and Jen Gore as alternates for this call and in the remaining days of absence.

Alternates not replacing a member are required to rename their line by adding 3 Zs to the beginning of their name and at the end in parenthesis affiliation – alternate, which means you are automatically pushed to the end of the queue. To rename in Zoom, hover over your name and click "Rename." Alternates are not allowed to engage in chat apart from private chat or use any other room's functionalities such as raising hands, agreeing or disagreeing. As a reminder, the alternate assignment form must be formalized by the way of the Google Assignment link. The link is available in all meeting invite e-mails.

Statements of Interest must be kept up to date. If anyone has any updates to share, please raise your hand or speak up now. Seeing or hearing no one, all documentation and information can be found on the EPDP wiki space.

Please remember to state your name before speaking. Recordings will be circulated on the mailing list and posted on the public wiki space shortly after the end of the call. With this, I'll turn it back over to our Chair, Janis Karklins. Please begin.

JANIS KARKLINS: Thank you, Terri. Hello, everyone. Welcome to the 12th meeting of EPDP Team. As usual, the first question is, whether the leadership proposed agenda could be accepted and followed during this meeting? I see no objections. We will do so. So, thank you very much.

The housekeeping issues, we have a number of them today. Let me start with the question on early inputs. We asked every group to review inputs from other groups and we discussed already in the previous call and it was suggested that maybe we could put this issue on the agenda of the team call for next meeting.

Question from my side is whether all groups feel being prepared for that discussion if that is organized next week, or more time is needed? I see no hands up. I assume that that might be acceptable. Now I see one hand. Marc Anderson, go ahead.

MARC ANDERSON: Good morning. It's Marc Anderson. Can you hear me okay?

JANIS KARKLINS: Yes, Marc.

MARC ANDERSON: Okay, great. To answer your question directly, I mean I don't have any issues with addressing the early input for review specifically. If the group thinks it worth us taking the time to specifically delve into that, that's fine. No objection. But that sort of differs from what I understood our plan of action to be with the early inputs. What I have understood previously was that staff would undertake to incorporate early input into our worksheets or workbooks, which I believe they have done, and then when we get to the appropriate points in each of those discussion items, we would consider the early input received from the stakeholder group, which to me which seems to negate the need to specifically discuss early input.

Again, I'm not objecting to this course of action. I'm just wanting to point out that this is a deviation for what I understood our path to be. If I understood it incorrectly, that's fine, that's my bad, but I just wanted to raise that.

JANIS KARKLINS: Thank you, Marc. The staff did its part of the job. Every early input has been added to the worksheets in their respective parts. But after proposing that I think two meetings ago, I got some comments and explicit request that these early inputs should be discussed by the team, and last week this request is confirmed. So hence, I'm asking whether all groups would be prepared to discuss early inputs next week, taking into account that this is a little bit quiet time and some team members enjoy their summer vacations.

I understand, Marc, you're not objecting and there's no further request, then I assume that we will put that on the agenda next week and would devote some time or we plan some time and then we'll see how active this conversation will be next week. So, thank you. That is then decided. Let's go to the next agenda item and that is – sorry, I cannot see on my screen.

That is proposed expert presentations during the lunch time at Los Angeles face-to-face meeting. Mark Sv proposed that some experts from Microsoft Digital Crime Investigation Unit would make a presentation on the way how they handle different cases in their daily activities. And after thinking when that would be, I proposed that maybe most appropriate would be during the lunch time as we had in Marrakech. That proposal was turned down by

some, and following the e-mail exchange prior the meeting, it seems to me that we could converge to the proposal, organize a special webinar devoted to the topic. And now, my question is whether that would be right course of action? Anyone wants to intervene? No hands up.

So, may I then take that Mark Sv with the assistance of the staff would prepare the webinar and we would schedule it at one classical time, maybe Tuesday. For those team members who would be interested in listening presentation and asking questions to experts from Microsoft. So, for the moment, no specific date, it depends on when we could organize that webinar. I see no hands up. I take that that is our common wish. Thank you.

Let us move to sub item C, Priority 2 small team meeting update. And if I may ask, Caitlin, to briefly introduce the sub point 1, and I believe also sub point 2. Caitlin, please.

CAITLIN TUBERGEN: Hi, Janis. I'm just going to share my screen. I'm hoping that everyone recognizes this document. It was circulated in July shortly after the Marrakech meeting. As you may remember, there were worksheets for all the Priority 2 topics and worksheet matches the format of the worksheet we've been going through for SSAD. There was one meeting that was pending following ICANN65 and that what the WHOIS accuracy topic. In terms of next steps on that topic specifically, the small team propose a briefing from Bird & Bird regarding its accuracy memo that it sent to the EPDP Team in Phase 1. And then, following that briefing the Legal Committee would review the draft questions that have

been submitted to determine if they should be forwarded to Bird & Bird.

As you might remember, the Legal Committee is currently reviewing Priority 1 questions which deals with the SSAD and following review of those questions, it will move on to looking at the Priority 2 topic questions submitted. This document was sent to the EPDP team and it shows all of the topics and all of the next steps proposed by the members that had attended those Priority 2 meetings.

We did receive some feedback from the Registrar Stakeholder Group on the next steps, although we didn't receive any feedback from any of the other groups. We're hoping that means that the other groups were okay with the next steps proposed. The next step is for the leadership team to look at this document and the next steps proposed by the small teams and send their proposal to the plenary team of how and when these topics will be handled. So, that's it for me, Janis. Thank you.

JANIS KARKLINS: Yeah. Thank you. Thank you, Caitlin. So, any questions. I see Amr has his hand up. Amr, please go ahead.

AMR ELSADR: Thanks, Janis. This is Amr. Just a clarification. My understanding was that the Priority 2 work stream issues were going to be – there's going to be a smaller group working on those and there would be an additional call each week. But eventually, they would report everything back to the plenary to review that

recommendations of sorts of how to proceed with these topics, and that there will be no presumption that all the groups agree to what the smaller group has come up with. So, I hope once work on these issues is done that the broader group could engage on whatever outcome comes of it. Thank you.

JANIS KARKLINS: Thank you, Amr. Your understanding is absolutely correct. Of course, the assumption behind the working in smaller groups is that their recommendations would be reviewed by all team with the positive mind. Otherwise, that would be just duplication of activities. So hence, that is the presumption. But of course if there is violent disagreement, what the small group comes up or proposes then of course that's a different story. I see Brian King is asking for the floor. Brian, please.

BRIAN KING: Sure. Thanks, Janis. This is Brian. And, Caitlin, thank you for that. I wonder if it'll be helpful since our colleagues in Registrar Stakeholder Group clearly have their act together and have submitted comments already on these worksheets. If it makes sense for the rest of us to do so in a given timeframe, would that be helpful before staff takes the next steps that you were talking about, Caitlin. And if so, what kind of timeframe does that look like or what path forward do you propose? Thanks.

JANIS KARKLINS: Thank you, Brian. Georgios, please.

GEORGIOS TSELENTIS: Yes, can you hear me?

JANIS KARKLINS: Yes, Georgios we hear you very well.

GEORGIOS TSELENTIS: Yes. Thank you. Caitlin, you just mentioned about a briefing regarding accuracy prior to a last evaluation of the questions that we have submitted. Do you have a set date for this one?

JANIS KARKLINS: Thank you, Georgios, for the question. Caitlin, would you like to respond?

CAITLIN TUBERGEN: Hi, Janis, if I could. I can try to address all of the questions that have come in so far, if I may. I'm starting with Georgios. Thanks for the question, Georgios. There's no schedule update for this webinar. That was just a proposal from the small team that thought it may be helpful to have a webinar or Q&A on that topic. And so, in the event that we move forward with that, of course the team will be notified and is expected to attend.

In terms of Brian's question which is thanking the Registrar Stakeholder Group for providing its feedback in a timely manner, the feedback on the worksheet that was on the screen as well as the Google Sheets which showed all of the feedback from the

small teams, that feedback was technically due in I believe July 11th, but seeing that some groups may have missed that deadline and also noting that this topic has been on our Any Other Business topic for the last few meetings but we've run out of time, I would propose if Janis agrees that we give everyone an additional week and I can resend those materials to everyone. So if you could provide that feedback by next week, by next Thursday, that would be helpful and then leadership could review all of the feedback and propose steps forward the following week.

And lastly, to address Amr's point. Amr, as Janis said agreed, small teams have agreed to amount to plenary consensus. I will note that when members of the small team did disagree, those disagreements have been noted in the Google Doc, so when the teams do review those documents, you'll see the differing opinions and you can provide additional feedback if you think anything has been missed.

Thank you, Janis. Back over to you.

JANIS KARKLINS: Yeah. Thank you, Caitlin. So with these explanations and proposed moving deadline for any comments on this worksheet and small group proposals by next Thursday, 15th of August, that we then look at them and I think that some time in Los Angeles will be devoted to the discussion on the way forward including how we should or could address the Priority 2 items, what would be the sequence and how would be the most rational way of doing that. So, may I take the absence of request for the floor now as agreement for this proposal? So it seems that is the case. We will

proceed as agreed. Let me now go to the agenda item update on Legal Committee.

LEÓN SANCHEZ: Hi, Janis, this is Leon. Do you want –

JANIS KARKLINS: Yes. Yes, please, Leon. If you could give us a brief update?

LEÓN SANCHEZ: Sure. Thank you, Janis. The Legal Committee had held its third meeting just the day before yesterday and the team has continued to review the different questions that were posed the Legal Committee. Some of the questions have already been redrafted and merged as discussed with the Legal Committee. There is one question that the group has agreed to forward to the Plenary for final sign off and pending no objection this would be forwarded to the outside council. This is question #7, it was posed by the BC and redrafted them by the BC again, so we will be sending this question for final sign off by the Plenary. If there are not objections then we would be submitting this question for Legal Council for Bird & Bird.

There are some questions that are still being redrafted and fine-tuned. We will be holding our next call in two weeks' time, and to that end we hope to have the finalized versions of all questions in order to evaluate them and hopefully have these final versions forwarded to the Plenary for final sign off and of course forward them if there are no objections to outside Legal Counsel.

So, that is the update on the Legal Committee. Janis, of course if there are any questions, I'm happy to answer them.

JANIS KARKLINS: Yeah. Thank you, Leon. Actually, I have one question. Whether you discuss that every time when Legal Committee would come to agreement to one specific question, you would forward that to the team or you would collect number of questions or team should collect number of questions coming out from Legal Committee and then examine them in one batch and then send them off? Have you had that discussion?

LEÓN SANCHEZ: Thank you, Janis. No, we haven't had that discussion but I think it would be practical to organize or to set up a question batches as you suggest, as it would be practical to be sending one by one question to external counsel. So, this is a good point that I will raise in our next call and I think that the logical way for us to act would be to build these batches and then have them forward for final sign off to the Plenary and if approved of course, send them to the external counsel.

JANIS KARKLINS: Thank you, Leon. I see Berry is asking the floor. Berry, please go ahead.

BERRY COBB: Hi, Janis. Berry Cobb for the record. I'll wait until this specific topic, it's just a quick administrative item.

JANIS KARKLINS: You are the only one in line for the moment.

BERRY COBB: Alright. Great. Alright. Thank you. Real quick, can someone on the line looks like a 4015 area code, San Francisco area ending in 776, can you please identify yourself?

ALEX DEACON: Yeah. Hi, it's Alex Deacon. Sorry for that.

BERRY COBB: Alright. Great. Thank you, Alex. Back to you, Janis.

JANIS KARKLINS: Thank you, Berry. So, any other comments or questions to Leon on the progress of the Legal Committee? I see none. So, then we will probably wait the next meeting of Legal Committee in two weeks' time, and then see whether there will be any further questions for the sign off for the team and we will put them on the agenda as they come. So with this, I think we have come to end of housekeeping issues and we could go to the use case.

The second and hopefully final reading of the case, investigation of criminal activity where domain names are used. Typical specific

example, phishing attack. So, you recall we devoted more than an hour for the first reading in the previous meeting and about half an hour in the meeting two weeks ago and SSAC, Greg has accommodated some of the comments and the proposals on Google Doc and I would like now to turn to Greg and ask him maybe to walk us through a little bit briefly to propose changes prior going into discussion.

GREG AARON: Okay. This is Greg. Thank you, Janis. I read the transcript for last week's meeting while I was away and I'd like to make a few high-level comments and talk about potential edits. Also, one of the things we discussed within our SSAC Team is some of these things are a little generic when we talk about them and it might make sense to offer specific case that we could walk through to make some of these things concrete and illustrate some of the principles involved. So, if people are willing, I do have a real life use case that would take about five minutes to walk through during our 45-minute segment. I do want to be cognizant of the time we have, so if people think that's useful, I think it would help people kind of sink their teeth into some of these issues and make some illustrations. But let's go to the kind of some of the general things.

In this use case, we're talking mainly about 6(f) issues. There's some discussion about – these use cases are to help us understand what's going on, provide examples. We probably don't want to slice some of these use cases too thinly. Some of the other basis on there might be relevant in some other use cases, so we did want to keep some of those on there. But for operational

security, we're mainly talking about third party requests, and so the 6(f) is going to be mainly relevant.

Tell you what, let's scroll back up. Let me just quickly look through the comments. Assessments of contact data. There is an issue of how this is done. When we're looking at the accuracy of contact data, I think there are two useful things to mention. One is that registrants do have the responsibility under their contracts to provide accurate contact information. The accuracy of the information is a factor in decision making, probably not the only one though. And this is not so much a case of gotchas where registrant may have made a mistake or something and those kinds of things do happen.

More what we're talking about here are pretty gross problems. For example, domain names registered to streets that do not exist. It's very common for us to see domain names registered to vacant lots, those kinds of things. So, it's a factor and sometimes you have a pretty gross violation, and those are the ones that we're especially concerned about. So, that's that. If we can scroll down, please, to the next comments?

I think I've talked about Task 3 there. Regarding Task 6, which is referring to law enforcement – and this also applies to when you're reporting an issue to say a registrar – you do need to say why there is a problem associated with the particular domain name and substantiate it.

Now, one of the things you want to do when you're talking to a registrar is you do want to say, "Look, we believe that there's a problem with this domain name." For example, the data may be

purposely falsified. Also, when you're reporting to law enforcement, you do need to get their attention as well. You need to tell them why you think there is a problem and substantiate it. Again, attribution is an important aspect to that.

Let scroll down some more please. Okay. As I said, lawful basis, we're mainly talking about 6(f). I'm not sure why 6(f) got lined through there. Okay, it's not. Okay, it's in the first paragraph. It's there. That's fine.

As we mentioned, tech address, we do have some tech contact information still in WHOIS as a result of Phase 1. And in some cases, security practitioners or responders are doing their work under contract to another party such as a victim. Okay, we have some edits here under 6(e), that's fine. Law enforcement, we'll talk more about 6(1)(d), such cases exist but they're fairly rare. And let's scroll down some more.

Safeguards. We felt obligated to put some information into the safeguards section but we're also cognizant that safeguard discussions are probably going to come later in the working groups discussions especially if we get into discussions of the basis under which the parties might be able to share data and whether some kinds of agreements are required. So, this is kind of some initial thinking but our feeling was we're going to get into this kind of detail later on as a group. I don't want to get too hung up on it. These are some ideas that have been discussed in the past going all the way back to the [cannoli] model over a year ago. One of the things that SSAC does want to keep in mind though is that whoever is receiving this data has to be obligated to use it responsibly and that use must take place within the law. So, I

don't want to get too hung up on the exact wording but the responsible use and the responsibility of having the data, retaining that for only specified purposes and for specified lengths of time and so forth is very important.

What I'd like to do is actually, if it's okay, go through a very short slide deck which I think the staff has. It's a real-life use case and it illustrates some of these principles. So if we could have that on screen, that'd be great. Thank you.

Okay. So, this is a phishing URL that came across my desk while we were sitting in session in Marrakech. Go back please to the first slide. And it caught my eye because it has my last name in it. It turned out it to be complete coincidence. But somebody on the mailing list I'm subscribed to said watch out, here is a phishing attach. Here is the URL. Go to the next slide please.

This is also displaying the background. I don't know if you can get rid of the – so, I'm actually showing this as a slide deck. So, I don't know if you can change that or not, but it's okay. What you see if you go to that URL, it was a phish against Georgia Tech. The staff probably and the students at Georgia Tech University, and you see it's asking for a user name and password and then you can get into personal accounts and have potential access to all kinds of personal information, financial functionality and so forth. So, that does not look good. Go to the next slide please.

Number three. Okay. Can we go to the next slide please? Thank you. There are other phishing URLs on that domain name. On a different URL, for example, we have this. Oops and we've lost it.

TERRI AGNEW: Sorry, one moment. I'm going to get that PDF version, so it's a view better. It'd be one moment.

GREG AARON: Okay, thanks.

TERRI AGNEW: One moment, it didn't save correctly. I'll leave this up and work on it. Go ahead, Greg.

GREG AARON: Okay. So, here's another URL on that same domain name. It's imitating Microsoft log in. This is a separate phish on the same domain name targeting Microsoft users. Next slide please.

Here is the WHOIS information for this domain name and here's what we can tell from it. We know that's registered at OVH which is one of the largest gTLD domain name registrars. The creation date on the domain was about a week before the phishing took place. Does that mean this is a malicious registration? No, not necessarily. The domain was probably entered into the zone as soon it was registered, probably with some default name server on it, so we don't know if the phisher registered this or if it was compromised in that week after registration.

So, creation date is interesting, it's pretty early but it's not determinative. We don't really have any contact information for it. Let's just leave it like this. We do have the registrant country

though, which is DZ. That is the country code of Algeria. This is not determinative. We don't want to block everything registered in Algeria of course, but relatively few gTLD domains are registered there. The name servers don't help a lot either, positivebenefits.co.uk was the domain name registered in 2011 and because it was registered years ago, it's probably some innocent registrant. There is one domain otherwise associated with it which is for hypnotherapist website, so we don't know what's going on here, we don't know if these name servers got compromised and the phishers has something to associated with it, but we have an old domain name here and that means that is probably not maliciously registered. This is not determinative either. Next slide please.

Okay. So if you do a DNS query you can find out where this domain is hosted. It's on this particular IP address, 139.99.73.130. And by looking at DNS records, we can also see what other domain names are hosted on that IP address. This is DNS information. This is how the DNS works. This is open information. Next slide please. Okay.

That IP address is run by OVH but it's a different division of OVH. It's their hosting division in Singapore. They have also hosting offices in Europe and in Canada. This is their information, so this might be where you would go to report this phish if you're going to the hosting provider. That's different than the registrar. Next slide please.

What other domain names are on that IP address? It's these set of domain names. Some of them look like the one we have a phish on which is in red. Some of them kind of look similar to the way

they're spelled and then some don't. One of the things we know about OVH is they do shared hosting. Many registrants sites and domain names may be put on the same IP address or sometimes one registrants domains will be on an IP address only, but we don't know the case here. So, the problem here is we've got this set of domain names, we want to know which others (the phishers) have registered potentially. But we can't tell without some of the contact information. And again, we want to be responsible. We don't want to block an innocent registrant's domain name. Also, we want to find out if these are maliciously registered, these are cases that we should send to the registrar because they can look at these other domain names as well. So we have this problem of potentially overblocking or underblocking. We also have the problem of ongoing harm. Do we want to let these other domain names sit there or do we want to have them addressed? Next slide.

One of the things we see is there was phishing on some of those domains before the Georgia Tech phish, in some cases several days before. So what we saw here is that the domain name with the Georgia Tech phishing on it was not taken care of for several days and then the phishing attack did appear on it. There are also domains in this set where phishing took place days after the Georgia Tech phish. Not only was this phish up but there is phishing on that set before and after, so there is potentially victimization going on over a period of time that did not need to take place but probably did, and this is not the situation we want. The removal of contact information from availability to be viewed for these purposes is allowing more victimization to take place. It's

allowing phish to come up when they don't need to, and that's a problem.

On the next slide we'll see that some took place several days even before this, it was phishing against Amazon. So, let's go to the last slide which is #10. The point here is that in some cases, there is information you can use in the set that's still publicly available. Sometimes name server information is useful, for example, but in this case, it's not determinative. The contact information in this case would've been incredibly useful for reporting, for preventing additional harm. Let's go to the last slide please, beyond this one. You want to respond appropriately, but in this case having contact information is really important to do that. You don't want to overblock or underblock. In this case, it's possible to respond proportionately. We can tell a registrar, for example, "You look like you do have some malicious registrations and here's what they are." A lot of times we will report things to registrars and they may take care of one domain name but not the others that are associated with it and that causes additional harm. In this case data minimization is possible in a few different ways. Looking to solve this problem might involve looking at a small set of domain names. We do not need to maintain a large database of what's going on in the entire namespace. We have a very particular problem, localized in a very particular place. Also, it might be possible to request information only in certain fields of the contact data, not necessarily needing all of it.

The bottom line here is alternatives that are available to us are not as effective. Milton, for example, said, "Go by registration date last week or go by nameservers." In this case. which is pretty typical,

that information is not determinative. It doesn't help us. But attribution, figuring out the registrant responsible is very important and GDPR Recital 49 says that looking at these kinds of things for this purpose is a legitimate interest.

So, let's bring down this information. I want to see if anyone has any questions.

JANIS KARKLINS: Yeah, Greg, there are many, many hands up. So, thank you very much for walking us through this case. Mark Sv, followed by Amr, and then Tatiana, and then followed by others. Mark Sv, please go ahead.

MARK SVANCAREK: Thanks. Mark Sv. Can you hear me?

JANIS KARKLINS: Yes, please go ahead.

MARK SVANCAREK: Thank you. Thanks, Greg, for this example. It demonstrates one of the things that I've been saying for a while that just because we're asking for contact data, it doesn't mean there are a lot of other things haven't been attempted before or it doesn't mean that we haven't tried other things, and so that is a helpful point. Also, this does not actually show what happens after this investigation happens which was going to be the topic of the DCU presentation. So, there are some places where you have to have that contact

information in order to go to the next step or the courts won't allow you to do it. So, thanks for this presentation. I guess that's it.

JANIS KARKLINS: Thank you very much. Amr, please.

AMR ELSADR: Thanks. This is Amr. And thank you, Greg. I had actually raised my hand earlier when you're going through the Google Doc which is back up on the screen. I appreciate that, Greg, you might not have had much time to go over some of the NCSGs comments that is, I was wondering if there was a way you would prefer we handle sort of a dialogue on some of them because a lot of what's in this use case NCSG members at the EPDP Team have found to be fairly problematic, at least raises significant questions. So, I'm open to whichever way you feel would be best to handle these at this point. I'm not sure if you've had a chance to look at all these comments in detail or not. Please go ahead.

GREG AARON: One approach we could take is since you've put notes in the Google Doc, would be for SSAC to respond in the Google Doc. That's what I proposed.

AMR ELSADR: That works for me. Thanks.

GREG AARON: Okay.

JANIS KARKLINS: And then hopefully the consensus will emerge or common understanding will emerge that would then take shape of the final document for this use case. Thank you. Next speaker is Tatiana, followed by Farzaneh.

TATIANA TROPINA: Thank you very much. Tatiana Tropina for the record. I actually want to respond to something Greg – thank you for your presentation, Greg. Covered in the comment of NCSG in his response to the comment of NCSG to Task 6 and I believe it also is related to his presentation. Greg talked briefly when he went through the document about the importance of attribution. Correct me if I'm wrong, I might remember wrong now because there was a presentation between his comment and my intervention. But there was something about attribution being important part of the process of reporting the incident to law enforcement like the notion that we put one needs this attribution. And I actually disagree as someone who is dealing with criminal law a lot. I do believe that law enforcement work and task is actually to provide the attribution. The entire work of law enforcement is to provide attribution and this entire work is regulated by the criminal procedural law. And I think in response of Greg to the Tasks 6 comment, there was a mix of sequence of steps and of actual frameworks of responsibility in criminal investigations, who does and what. And I do believe that we are creating causality dilemmas when there is none at all attribution for the purpose of

crime investigation is actually the domain of law enforcement. Because it is them who have to apply the safeguards as provided by the criminal procedural law and they have a framework of accountability for this which private companies do not have.

And so, I do not believe here in the argument that it is an obligation or it's sole obligation to attribute before reporting the incident to law enforcement. I do believe that, okay, crime has not to be reported as a mere clue. Of course, more information has to be reported but law enforcement started investigation just fine and demand personal data. And I also believe that there is an issue of applicability of the Recital 50 because it applies only if the personal data is in the possession of the controller or they are transmitted to the competent authority which private investigators, so private industry are not. So I doubt there is really applicability of the Recital 50. I think NCSG also put in the comment but I think that at least not for the purpose of attribution and not at all. Thank you very much.

GREG AARON: Okay. Thank you for that comment.

JANIS KARKLINS: Thank you, Tatiana.

GREG AARON: There are probably two ways to define attribution or maybe two levels. One is to say there is a party. We have identified that is perpetrating these acts. Whether or not that name is accurate or

not, that's one thing. But in one case, we'd say, "Look, there's one party responsible for all this activity, these multiple domain names." We may not know the real identity but at least we've attributed it to a particular party. Now, the criminal investigator is going to try to find out the identity of an individual, which might be I'd say a deeper level of attribution.

But I will point out a very practical issue which is that law enforcement doesn't – and prosecutors don't even take on cases unless they feel like they've got something to go on and their case is large enough to devote to resources too. So, attribution by researchers and security people is actually really important because they're the ones who say, "I have seen this issue and it is associated with a particular party." So, I'm going to disagree that attribution is only for law enforcement. It is performed as a practical matter by private parties.

Milton Mueller, for example, wrote a whitepaper recently saying – actually a lot of these cases, it is done by private parties by looking at cases that were either written in the press or came out through cases that were eventually filed. Thanks.

JANIS KARKLINS: Thank you, Greg. We have still many people in line. Let me now turn to James Bladel, followed by Margie.

JAMES BLADEL: Hey, thanks. First off, I just wanted to say thanks to Greg and SSAC for putting this together. It's always helpful to have some concrete examples to cut through some of the abstract topics that

we're wrestling with. Just general reactions and then I'll drop out of the queue because I see it's fairly long and we're short on time.

I don't think anyone challenges the idea that more data points allow for a more comprehensive and effective investigation and mitigation of harms. That's the balance I think we're trying to strike. What I didn't hear too much about was whether or not pseudonymized data responses could be used similarly to replace the release of actual personal information that might be covered because I think Greg, as you and others are aware, unlike say law enforcement, there are no credentials or bonafide or whatever that we can check that a cybersecurity person or organization is who they say they are, I understand that overblocking and underblocking may be aspirational. Overblocking happens all the time. So we're trying to I think minimize not only the potential harms of overenforcement of casting too wide of a net but also the harms of releasing information that might contribute to – that might be a wild goose chase for investigators like this.

I'll just drop out of the queue. Those are just some of the thoughts I had. Otherwise, I thought it was a good presentation. Thanks.

GREG AARON: Okay. Thanks, James. I'll respond very briefly. We do believe that an accreditation program would be possible in that it is going to be possible to find out whether a party has the professional expertise experience and legitimate interests in the topic. The pseudonymous data is maybe something for another time when we have some more time to talk about it. It is an interesting idea

but it also poses some challenges and maybe let's put a pin in that for later.

JANIS KARKLINS: Thank you, Greg. Next in line is Margie.

MARGIE MILAM: Greg, thank you very much for this presentation. I think it really highlights a lot of the issues that we'll scope out some of the use cases that the DC presented. A couple of things I wanted to highlight and focus on is if you look at the example that you just gave – essentially you started with one domain name and you ended up needing to get access for say 20 domain names. That's just one phishing event. What I think this group needs to really understand is large platforms and major providers of access of the kinds like say Microsoft, Facebook, and others have this at huge scale. So what we really have to focus on when we talk about the access is the volume and the attribution because as Greg mentioned, this is not something they get solved by LEA only. In fact, it is the major companies that are doing it to protect their platforms, to protect their customers, to protect their brand, and there's also legal requirements that relate to that as well. So that has to be kept in mind as we scope this out.

The attribution in particular is important because when you have so many domain names that you need to assess the risk, if you see some that are tied to a network and link to prior phishing event – and this is where the attribution is really important – that's what shows you where to focus your resources and that's where

you make the decisions on whether or not you feel like you should actually go to court and go after the actual individual or network behind those attacks. We just have to be careful here. As we create the WHOIS policy that we don't prevent and prohibit that kind of activity, that kind of activity from some sort of maybe trusted informant like our credited cybersecurity professional. Whatever it is, we'll get to. It needs to be high volume and it also needs to be very quick.

This is the reason why you'll hear us pushing back very hard on manual review of all of these requests. If you can imagine, Alan Woods and others, registries/registrars, trying to figure out on a case by case basis, whether they need to look at every single request, it will simply not scale. The ability to take this stuff down quickly so that actually individuals' personal information is not stolen and the financial information is not compromised is something that I think we have to recognize and ensure that we build the policy that allows us to continue to do the good work to prevent those things from happening.

JANIS KARKLINS: Thank you, Margie. Next in line is Mark Sv, followed by Chris.

MARK SVANCAREK: Thanks. I had a couple of points. One, I think there is some mention about criminal versus civil, I am not a lawyer but I thought that the example given was actually a civil case. So, just throwing that out there. There was a mention earlier, so you're in the queue for a while. Sometimes things overtake you.

About the private investigators, I think Greg mentioned that a large number of these things do start with the private investigators because the police don't have the resources and you have to bring forward something pretty compelling before they will get involved.

To Tatiana's point, those are exactly the kind of questions that you should ask during the webinar with our DCU because they can answer them. That was the intent of that, not to just show that, hey, things got harder. Just to understand the reality of the process. Not making a point one way or the other.

Second, pseudonymization. I think that will work in some cases, not in other cases. I mean if you're talking to a registry, I am told at least that the way that the records are done at that level, they won't actually be able to – if you wind up with a bunch of things that are hashed differently then you can't actually match. So, it will probably work in some cases, not in other cases.

James, thanks for mentioning how you know who a cybersecurity operator is because that's going to be a really serious point. In the past we didn't have to do that and now it's going to be critical how can you trust them. Another thing that DC would've talked about is how we make those guarantees to the police or to the courts and when we have to put forward bond even.

Finally, there's a question about attribution to individuals versus states. Last week James told me not to tell anymore anecdotes but in the anecdote I was going to tell, that was a case of bank fraud. That was a case where the attributions being done to a criminal gang as opposed to state actor. Thanks.

GREG AARON: Just briefly, thanks for these comments. I personally would like to hear from Microsoft DCC. They're an example of an organization that got a court order that allowed them to suspend domain names that get certain kinds of things done as they found the domain names. Not just a list that a judge approved but judge gave them the ability to do some things on an ongoing basis as they found things because things were such a timely problem.

In this case, by the way, this could be a civil or a criminal issue. Phishing is a criminal activity. It is theft, it is fraud. It could also be pursued by private party who is the target but it's also a criminal issue. Thanks.

JANIS KARKLINS: Thank you, Greg. We have three further requests. Chris. Alan, Alan Woods, and then Hadia. Chris?

CHRIS LEWIS-EVANS: Hi, Janis. I just want to go back to Tatiana's thing about attribution. I think Greg here is talking about a different sort of attribution. Certainly, when we're talking about reporting to law enforcement – and I think as Mark just said – what our law enforcement agency would like to see is the way you have seen multiple cases of phishing and some scale of impact to a number of victims. That gives us quite a lot more to go on, so I think the way that SSAC have used attribution here is our attribution to some malicious actor which they then might want to report to law enforcement.

I think there's two very different things which is attribution of a natural person and attribution of actor that has a collection of domain name. So it might be quite interesting for us to just [inaudible] that and maybe not confuse it or mix the two up, which I think is not what we want. I'm going from the comments in the text here. I think that's quite an important differentiation when we do the attribution that finding a group of all the malicious activity is very important that you might not necessarily want to actually identify a natural person, which brings on the second point which is as James raised around the pseudonymization, I think it could apply here quite nicely. But as Greg says, there's a number of points we need to bear in mind. One of those is you would lose one of the aspects that you would look at the data for which is, is it fake? Because you wouldn't be able to see that within an anonymization which might say if it is a compromised host or a malicious host. So you would lose that level of awareness. Then also the anonymization would have to go across all of the TLDs so that all of the registries and all of the registrars to be really useful. That's certainly one of the problems but probably best not for now. Thank you.

JANIS KARKLINS: Thank you, Chris. Alan Woods, please.

ALAN WOODS: Thank you. Actually, I see what I'm about to say is actually being hashed now currently in the chat but I'll go through it anyway. Thank you, Greg, for that. I do personally think that this actually

goes through the core of what my e-mail this morning about the Microsoft presenting to us.

I think what you highlighted is the fact that the law has changed and we've caught up with the law and it's more difficult for you to do this. Don't think there's anybody suggesting that it's not more difficult. I don't think anybody on this call would disagree with the fact that easier access to the data for the right reasons or something to be absolutely sought after, because again just streamline those processes. So I think that I understand where it's coming from but I still see very little value in going to that, specifically on this because it doesn't change the fact that the law is how the law is written and we have to make sure that we are within the boundaries of law.

Again, Margie, I completely agree. I do not want to have 15,000 daily report requests from a complete [inaudible] outside of the registration that I deal with on a day-in day-out basis because I don't have the way to do that. But at the same time, again, I just have to deal with the fact that this is the way the law is. Our entire industry has developed around what was an effective misapplication of the law and we need to now adapt to that.

So we're all focusing on the same thing here. We're all trying to get to make this easier and better but not crossing the line that is what is legal or not. I'm just at the end. I just want to bring this right back to what are we trying to achieve with these use cases? I think what Greg has set up very well there is that he'd gone through all this process, all this information that he has said, "I have done in this previous post. I put this investigation thought into this and now is the point of which it could be really helpful for

me to actually get that additional data." Even though it's going through this thing is not possibly anything other than that 6(1)(f) [inaudible] 6(1)(f). We will wait for the Bird & Bird to come back on that one. But that is the basis of a 6 (1)(f) request. I have done all these by taking all these steps, and now this is the balancing test. We believe that this is the next necessary step. That would be something that will allow to [inaudible]. We need to bring this in. Scaling things that are very important for us to actually consider but at the same time, we don't know the way the law is lined and we have to be somewhat conservative at this point. We develop over time.

I just want to say thank you again. I agree with you all. I don't know what you're saying but let's be honest. What we're trying to do here is streamline the way that the process will run. Everything you said there to me is just the 6(1)(f) process. What we need to consider in a 6(1)(f). I don't know if we need to be going down really to that detail because that is up to the requestor at the end of the day to go with that detail, to allow us to come to that decision better. Thank you.

JANIS KARKLINS: Thank you, Alan, for this comment. Next is Hadia.

HADIA ELMINIAWI: I would like to quickly thank Greg and the SSAC Team for this use case. From an end user's perspective, this is very important. I thank Greg also for the example that he gave us and it's sad to

know that there might have been victims and that this could've been avoided.

I would like also to quickly note that I can't imagine this done manually. You will need a team of people doing nothing but that. I also don't see any contradiction between what GDPR requires and the automation of such process. Thanks again and I assure that this is very important from an end user's perspective. Thank you.

JANIS KARKLINS: Thank you, Hadia. I see Mark Sv's hand up again. Is it old hand or new hand, Mark?

MARK SVANCAREK: It's a new hand because –

JANIS KARKLINS: Okay. But then small hand please, quick hand.

MARK SVANCAREK: Okay, yeah. Greg mentioned something, I just wanted to tap in on it. It is true that the initial search might be a 6(1)(f) but there are some cases where having brought the evidence forward as Greg mentioned, the court may have point a special masters or some equivalent thing which would give us the ability to do more far ranging searches which might be performed under a different basis. I don't want to go into too much detail on that because I'm not a subject matter expert. So, just a data point.

JANIS KARKLINS: Thank you very much, Mark. Thank you, everyone, for this input in the discussion. For me, what is important that by putting forward our thoughts and arguments we're learning and developing understanding how these things work in real world that would help us ultimately to also formulate policy recommendations. I think this is time wisely spent. So now the question is how will we proceed from here? Since time is flying and we want to also look at the second case on what ALAC has proposed, let me maybe ask very quickly. If we are looking to Section B on all tasks performed, is there any violent opposition to those tasks as they have been maybe fine-tuned in the new version of the document?

The same. I see no hands up. The same question on data elements. I think we came to a kind of conclusion that not necessarily all data elements that are mentioned here would be required nonsystematic basis. Marc Anderson?

MARC ANDERSON: Hi. I'm sorry. I think I'm a little bit lost. Can you please clarify like where we are and what were you reviewing at the moment?

JANIS KARKLINS: I was asking whether there is anyone from the team violently opposing entries in Subsection B on those formulated or explained six tasks that private investigators would perform.

MARC ANDERSON: Okay. So I see the use case. But you're asking specifically for feedback on the use case document that Greg just presented?

JANIS KARKLINS: Yes.

MARC ANDERSON: Thank you. That was the missing piece of the puzzle for me. Thank you.

JANIS KARKLINS: So, will we continue or you're fine with that? So no request. The same question is about Subsection C which speaks about the typical data element that would be disclosed, with understanding that that would not be requested on systematic basis. Greg, your hand was up. Or was that a mistake?

GREG AARON: It's down.

JANIS KARKLINS: Okay. On data elements, no comments? On lawful basis, I think that provided edit is very clear and correspondence to the concerns that have been expressed last time last week.

Since Subsection E is just more explanation to Subsection D, any opposition or violent disagreement what was written in Subsection E? Chris Lewis-Evans?

CHRIS LEWIS-EVANS: Sorry. I have to get off mute. The 6(1)(b) I still have massive problem with. Realistically, it's indicating criminal acts before it getting to threat to life. I think before you get to a threat to life situation, you have an obligation under or you would be acting under one of the other legal basis before hopefully got to a threat to life situation. So, I think realistically, when you come to do your determination around which is the right lawful basis, you should realistically be [inaudible] before you get to a threat to life situation. Thank you.

JANIS KARKLINS: Thank you, Chris. I will take Farzaneh before giving the floor to Greg. Farzaneh, please.

FARZANEH BADII: Thank you. I think that you are going through the document [inaudible] final reading. Are you going to approve this at the end of the meeting? Because a lot of our comments on this document were not addressed and we cannot do the final remit without our comments being addressed. Just one thing.

If you want, I can just read through our comments. I will go through it. But for the interest of time, it might be better as been said to just respond to our comments later. Thank you.

JANIS KARKLINS: Yes, Farzaneh. It's not the final reading. It seems we cannot get the final reading. Today no approval is expected at the end. We will continue exchanges of opinions on Google Doc. Before we will ask Greg to make a final shortened and present the document in its final version. Margie, please.

MARGIE MILAM: Hi. I just wanted to point out that we're still seeking legal advice from Bird & Bird on some of the legal bases. I think anything that talks about the legal bases in these use cases would be subject to revision once we get the legal advice from Bird & Bird.

JANIS KARKLINS: Understood. Thank you. Milton?

MILTON MUELLER: Milton Miller here, Georgia Tech. I'm looking at Section E and I'm just wondering whether this has gotten somehow mixed up with two different use cases here because what's happening with Section E is that this use case which was deliberately supposed to be about private actors doing investigations of problems that they're having is slipping over into law enforcement. I think one of the important things about these use cases is to keep those things distinct. So I just see confusion rampant in Section E between is this a private actor or is this some kind governmental actor? Cases involving child sexual abuse, human trafficking, suicide, missing persons – this is all law enforcement activity. In what sense is Microsoft or Facebook going to be initiating investigations on these kinds of things? I can understand how they might report

suspected activities to law enforcement but these are law enforcement activities and it says rather explicitly in this added language, these cases would apply in investigations carried out by designated and authorized organizations such as national CERTs or in cases where the investigator is officially authorized or contracted to perform those functions. So let's clarify this. What is going on here? This is a confusion with another use case which we've already discussed. That's all.

JANIS KARKLINS: Thank you, Milton. Greg, please take that note seriously. This subsection should be probably seriously reworked. But let me first ask Amr to provide his comments.

AMR ELSADR: Thanks, Janis. I wanted to point out a couple of things here. First, the examples provided in the first bullet on top would refer to the legal basis of 6(1)(a), (b), and (c) where the data subject or the victim are customers or business partners of the investigating entity. I'm not clear on why you need a legal basis to access this data to begin with. GDPR provides the right for the data subject to access its own data any time. So if the investigating entity is a customer or a business partner of the data subject which is in this case supposedly a victim, I don't see what the relevance of these legal bases are or how are they applicable.

In the third sub bullet below that – sorry, the second one, which refers to Recital 47, preventing fraud constitutes a legitimate interest on the part of the controller. This I think is applicable to

6(1)(f), not to 6(1)(a), (b), or (c) unless I'm mistaken, Again, this is something else that kind of confuse me here.

Let's see, my last comment … the second bullet which starts with 6(1)(d), those are clearly cases that need to be investigated. But again, I'm not sure how 6(1)(d) is applicable and I don't see how any of the legal bases over here sort of support disclosure to a non-LEA investigator. I think this also applies to 6(1)(c) in the third sub bullet to the first bullet. 6(1)(c), if I'm not mistaken, refers to a legal obligation on the part of the controller. Again, I don't see how there could be a legal obligation on the part of the controller to disclose data to an independent investigator. Again, we're not talking about a competent authority here. We're talking about a non-LEA investigator. So if 6(1)(c) is applicable, it wouldn't be in this use case, I would imagine. All of these just add up in my head to why 6(1)(f) is the only legal basis that should be applicable in this use case. But then, this whole Section E would need to be revised if there was agreement on that. Thank you.

JANIS KARKLINS: Please go ahead.

GREG AARON: I was going to say thanks for the comments. We'll take those into consideration. One thing that we're thinking about is that there are various legal obligations and contracts in place sometimes. For example, if you're a registrar, you don't do your own credit card processing. You pass that information to a party that does it for you under contract. Some of these contracts may have legal

obligations associated with them. That's why (1)(c) is there. We probably don't know everything that's involved here so we put that there because it might be important.

We'll take those things into account. My action item is to go through this document, respond to comments. Janis can then decide how to put it up for a last call. Also, Janis, as a point of order, Milton has been identifying himself as Milton from Georgia Tech. I'm pretty sure he's not representing Georgia Tech in these proceedings. Thanks.

JANIS KARKLINS: Thank you, Greg. We still need to go through other subsections just to collect violent opposition, but as you rightly suggested that my proposal will be to ask you to revise the document by using Google Doc responding to our comments. So maybe do a few iterations back and forth until there is convergence to a certain formulation, and then present the revised document for the team. Again, I don't think we were talking about formal approval. We're talking about going through everyone feeling more or less comfortable with the document because we're not sort of fine-tuning use cases per se but we're trying to extract from discussions about those use cases our understanding what the policy recommendations might be. This discussion of use cases is just the method to extract those grains and put them in the Policy Recommendation document that hopefully we will see in its zero version at Los Angeles meeting.

Let me now very quickly ask on sections of safeguards. Is there any violent opposition? I'm referring to Subsections F, G, and H. Farzaneh, please.

FARZANEH BADII: Thank you, Janis. This is my personal comment. I am confused as regards to how we interpret safeguards applicable to the disclosing entities and the requirements because if we are talking about safeguards that should be considered to protect their data subject by the disclosing entities who are involved then we need to talk about mechanisms and requirements [inaudible] the data subject.

However, in this use case specifically, I see that there are requirements to facilitate the disclosure to the third party and in a way serve the third party interest. I just want to know how do we interpret these safeguards? Because I thought that the safeguards were there in order to protect the data subject and not these not requirements to facilitate the disclosure. Of course, we are going to discuss that but I don't think that they should be mentioned here as I mentioned. Just a clarification would be great. Thank you.

JANIS KARKLINS: Thank you, Farzaneh. Again, as I said, these reflections, safeguards, they represent the input to build our understanding on different aspects related to actions of requester and potential actions of the data holder or registry/registrar. These tables, we'll not find directly the reflection in the policy recommendation as you can imagine. But they simply help us structure our thinking about

those topics. Some of those topics are specifically required by our Charter to go through and this is just how we fine-tune our own understanding. At least this is how I see our activity.

On accreditation, I think we had already exchanged. On automation, very end of the table. Any comments on Subsection N? Alan Woods?

ALAN WOODS: Thank you. Honestly, I think it's worth to just say on the record that this is again one of those very core based legal questions that need to be answered. I think we should probably listen to Bird & Bird on that one. For argument's sake I do disagree. Some automation is likely a very possible thing in this. But again, we could be [bringing that].

JANIS KARKLINS: Thank you, Alan. Volker?

VOLKER GREIMANN: Yes, thank you. I think we should qualify this authorization is necessary as believed necessary by some parties and believed impossible by others. I think that's something that as Alan rightly said, the legal review will have to result in not something that we should just assert in this document at this time. It's very questionable at this time, so we should qualify it before we move on. Thank you.

JANIS KARKLINS: Okay. Thank you. I think we now can draw the line on the reading of this particular case at this moment. As I suggested, I would ask Greg and SSAC Team to work in response to comments on Google Doc and then maybe go in few rounds until the common ground emerges, and after that to do fine tuning of the document itself with the final proposal for the final reading. We would take it up if ready next time or a week after. Would that be okay? Greg, ready?

GREG AARON: Yes. That sounds great. Thanks to everyone for their comments. Much appreciated.

JANIS KARKLINS: Thank you very much. Let us move then to the next item on our agenda, and that is online buyers identification and validation of the source or services/ Internet users validating the legitimacy of an e-mail or a website to protect themselves.

ALAC case. We had a reading of first subsections last week. We didn't finish it. If Alan or Hadia can remind where did we stop last time – it escapes my memory for the moment – that we could resume our further reading from that place. Alan, please. Alan Greenberg, your hand is up. Alan, we do not hear you if you are talking.

ALAN GREENBERG: Can you hear me now?

JANIS KARKLINS: Yes. Now we can hear you.

ALAN GREENBERG: Alright. My Zoom has kept on dropping so my phone is not necessarily synchronized with my screen so I couldn't tell whether I was muted or not.

A couple of things. I really don't know where we stopped but I'd like to make a couple of general comments. The whole issue of legal versus natural person is one that we have to come back to in this group and we haven't, and a large part of this use case focuses on that. The use case is presuming that we will not change the legal versus natural and therefore, it is still a relevant issue that although GDPR does not protect legal persons, the RDS database itself may not be particularly forthcoming on whether this is a legal person or a natural person. The use case makes that assumption. If indeed we end up identifying natural persons and legal persons definitively in the RDS then we have a completely separate situation, but we haven't made that decision yet so we're assuming the status quo will change. There is no question that a data requester who is not identifiable and is asking for information which is clearly asking to reveal natural person information is not going to get it in this kind of circumstances, not without being able to demonstrate that some harm has been done and make a case to the controller.

I just wanted to make that statement to begin with because we're in a fuzzy situation here and I think to some extent we're talking at

cross-purposes when we're looking at whether these are valid use cases that have some reasonable expectation of getting answers or are just looking to obliterate GDPR and make it invalid, which was not the original case. In that context, wherever we are, we should continue. But I really don't know how far we got last time. Thank you.

JANIS KARKLINS: Thank you. Hadia?

HADIA ELMINIAWI: First, I do agree totally with Alan and I would repeat what he said. If we actually had this distinction between the legal and natural persons, we wouldn't have needed to present this case. I would like also to note in the beginning that this use case is not about curious users and James put in the public comment, put in his comments on the use case that public consumer protection authorities already have those rights and do it, and this is true. However, this case gives an opportunity to end users to be a force of good in the electronic marketplace. It enables the responsible users. It also enhances a trust in the e-market and enables competition where the user don't necessarily need to go to well-known names and sites. I would defer again to a policy paper by the Organization for Economic Cooperation and Development that actually said, "Easy identification of online businesses is a key element for building consumer trust in the electronic marketplace."

I think we quickly went through the whole case the last time but I would start from the lawful basis of entity disclosing nonpublic

registration data to the requester, which is 6(1)(f) and Recital 47 says, “The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned.”

I would underline the word “preventing fraud.” This is actually before it happens and not after. This may be a response to what Milton was saying at some point that we should consider such cases after actually we have a victim. But again, GDPR encourages to do otherwise and help prevent rather than to start investigating after having actual victims.

Supporting info to determine lawful basis for the requester. As I said, it’s Recital 47. Because we are based on 6(1)(f), we have the purpose and the necessity and the balancing test and the purposes of fraud prevention. Again, if you're trying to purchase a good or acquiring a service online, I gave an example but I actually said before with regards to buying, for example, an online ticket. If you don’t go to one of the well-known sites because maybe another site gives you a more competitive price and you booked your ticket and you can check online, you see it reserved, but the whole amount maybe hasn’t been – and this is an actual case. What I’m saying is an actual case. Your credit card has just been verified but the whole amount hasn’t been deducted. Then you receive an e-mail from the website saying, “We reserved your online ticket. It hasn’t been ticketed yet. In order to confirm it, we need a photo of your ID and your credit card.” You might think, “I’m booking an online ticket and maybe they do need a photo of my ID.” You check the airline and you find your ticket is not confirmed but it’s booked. But then you're not sure. They say, “If

you do not respond before this time, we cancel your ticket." So you might provide the information or you might think, "No. I would like to get more information about this website." And this is where you go and try to go through WHOIS which doesn't exist anymore and that's good because of privacy reasons. But you need to have a path or a mechanism through which you can verify the e-mail you got or the website that you are purchasing the ticket from. Or you can simply decide to cancel your purchase, and this is good as well.

This path or mechanism for end users to be able to verify the e-mail or the domain name, it doesn't necessarily mean that information will be disclosed to the requester. It's based on the information they provide. And definitely there has to be safeguards and ways to validate that the information that the user is providing is correct.

Again, we're not envisioning here any kind of automation or accreditation but we think that such a path is necessary to give responsible users the chance to be proactive.

JANIS KARKLINS: Thank you, Hadia.

HADIA ELMINIAWI: Okay. Then the balancing test, of course Recital 47 says, "At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place."

Definitely if you're talking about a commercial website, they do expect that. This is with regards to the lawful basis and then the safeguards applicable to the requester. Of course, they first provide the name, the reasons for this request, the information that there is no other means through which this information could be obtained and agreed to use the information for the purpose it's required for. Again, it is not necessary to have complete information about the data subject. What's necessary is to have a legitimate means through which the consumers could actually contact the data subject and verify their activity. Safeguards applicable to the data subject – all safeguards given under the GDPR definitely. There is no need for Boolean search. It requires only for current data of course.

And accreditation now, we don't envision any kind of accreditation or automation.

What information is required to be provided for a request under this lawful basis? The contact information, but again, it doesn't have to be contact information. What we are asking for is a means through which the data subject can contact and validate the activity.

Expected timing of substantive …? As soon as possible. Instant acknowledgment of course, and then as soon as possible.

JANIS KARKLINS: Hadia, thank you very much. I think you did introduction of this case already last meeting.

HADIA ELMINIAWI: Yes. I think we're covering it all.

JANIS KARKLINS: It sounds to me a little bit like that.

HADIA ELMINIAWI: Yeah, that's it. I'm happy to answer any questions. Thank you.

JANIS KARKLINS: Yeah, we have a few hands up starting with James Bladel and followed by Stephanie. James, please go ahead.

JAMES BLADEL: Thank you, Janis. Thank you, Hadia and ALAC, for putting this together and walking us through it. A lot of reactions here but I think just generally that what you are describing in some cases is consumer trust, consumer confidence, commercial integrity of commercial transactions, and the ability to essentially verify the integrity of the website – all of these, in my opinion, is out of scope of what we are trying to do because we continue to reference websites and some competitive issues associated with websites, the first problem is that RDS does not link contact information to websites. RDS information, of course, is associated with domain names and there's not an iron clad one-to-one relationship between domain names and websites. Multiple domain names can point to single website and vice versa. Multiple websites can operate under a single domain name or domain name could be a marketplace of websites, multiple buyers and sellers coming

together. So this is not an association where I think RDS is a useful tool for achieving what you have described.

Secondly, there are existing tools, whether it is SSL, Better Business Bureau, Yelp, for example, or other price monitoring or complaints type services, all of those currently exist as commercial alternatives to what's been described in this particular use case.

Then finally, I just want to point out – and I think this goes to the heart of our comment on behalf of registrars – is that there are two types of folks who would be engaged in this, you mentioned, curious users would not have access to this. And we note that individuals and groups who are sponsored by legislation or who have legal authority to pursue these types of interest already have other use cases. So the only folks who would be left to exercise this use case would be curious users and therefore, they would not qualify to have this sort of personal information.

I think the registrar comment stands. We believe that when you take the legitimate parts of this use case and put them in their proper home in other use cases that what is left does not rise to the threshold of gaining a legitimate use case, and so therefore this use case is either redundant or unnecessary. Thank you.

JANIS KARKLINS: Thank you, James. Stephanie is next.

STEPHANIE PERRIN: Apologies for the delay in unmuting. James has said most of what I wanted to say. So I'm going to restrict myself to a remark that I think I made last time at the introduction here. I'm possible sort of thinking back to being a former government person looking at consumer protection issues on the Internet. I just want to stress that I think it is profoundly irresponsible not only for ICANN to attempt to step in here and assume the mantle of being responsible for consumer protection for what goes on a domain name after they have granted it. I know I've been told that the horses already left the barn on that one or are already doing trademark rules. Sure, but that's a lot closer associated to a domain name. This is not. This is the reliability of the individual or entity that is operating a website and to encourage consumers in any way to look to the WHOIS directory – let's call it that for shorthand – at the WHOIS data. To determine the reliability, when the ecosystem is as complex and multilayered and filled with things such as privacy proxy, such as resellers, is absolutely irresponsible. Consumers should not be looking at WHOIS. Period. The curious, fine, go look at WHOIS. But does it tell you whether the operator of that website is going to be a crook? Has a good reputation? Can be trusted? Absolutely not. We as a society should be encouraging people to look to the proper places such as their browser and their security monitoring, etc. I really feel quite passionately about this. It's irresponsible and we should stop doing it. Thank you.

JANIS KARKLINS: Thank you, Stephanie. I would like to remind we have 10 minutes and we still have a number of hands up. I would like really now to

draw the line under the list: Farzaneh, Margie, Mark Sv, Greg, and then Alan Greenberg. That would be for today.

FARZANEH BADII: Thank you, Janis. I'm going to be really short because others just covered the points I wanted to make. I think a more systematic way of arguing for access to WHOIS is needed. I think in this use case, we can see that there are a variety of ways to actually verify the integrity of a website and GDPR says that only when it is necessary you should be able to access the personal information of the data subject.

I think the necessity is not fulfilled here. It's obvious because there are many more ways than having access to a personal data to verify the integrity. I don't see the necessity being proven and there are alternatives to it, so this use case I think it should be deleted and not considered. Thank you.

JANIS KARKLINS: Thank you. Margie, please.

MARGIE MILAM: Sorry, can you hear me?

JANIS KARKLINS: Yeah, we can hear you.

MARGIE MILAM: Yeah, I disagree with a number of statements regarding the scope of what we're looking at. The Bylaws of ICANN are not as restrictive as the others mentioned. In fact, that's why we have the consumer choice competition, trust review because some of these issues are certainly within the mandate of ICANN. But one of the things I wanted to highlight and suggest that we look at is the notion that perhaps this could be limited to legal persons. If you think about it, when registrars receiving their request and they have access to the contact information and they could look at it and see whether it's clearly a legal person and whether or not the information is reflective of some major commercial website. Imagine eBay as an example. From what I think ALAC has done is they made this manual thing which I think is correct in this case. I think that there is probably an ability to do the balancing test so that it does weigh in favor of the consumer when the website is clearly a commercial website. So I think there's a lot of merit here. I think we should explore it and see if we could come up with some sort of policy recommendation around it. Thank you.

JANIS KARKLINS: Thank you, Margie. Mark Sv, please.

MARK SVANCAREK: I want to agree with some other people who've already been on here that I'm really skeptical of this use case where it applies to individual consumers and curious people and stuff like that. I think it's really only applicable in cases where there's some sort of large scale reputation system that's going on and there's a lot of factors that would go into the reputation. I think that registrar and who the

privacy proxy operator is probably weigh more than the personal information. But whether or not you have personal information, would just simply be a data point that would weigh in to that factor. So if you made a request and it was denied, okay, that's a data point. Thanks.

JANIS KARKLINS: Thank you. Greg Aaron?

GREG AARON: To emphasize what Margie has said, the ICANN Bylaws say that when we engage in this policy making process, we do have to consider and ascertain the global public interest. That's a general kind of a thing which is what's useful for the public and in their interest. Now, there's a great deal of division I've thought about what exactly that involves, but it is also different from public policy which is what governments and public authorities decide. So it's our responsibility to consider these kinds of things. I think looking at this use case is a legitimate thing to do. We may come to some decisions about it.

The other thing is that it goes back to what Alan said which is, "The law does not protect legal persons. GDPR protects the data of individuals." Right now we do have a situation and SSAC has stated that is an over application of the law. And we do have this issue of whether companies are putting the contact information of individuals into their domain name contact records. But that's perhaps not a Super Bowl problem. But right now SSAC believes that the data for legal individuals might be able to be straightened

out and would therefore be in the public record and you would not have this issue of people looking at it because it's not protected. Thanks.

JANIS KARKLINS: Thank you, Greg. I draw the line after Alan. In the meantime we have additional three hands up. We have only five minutes. Unfortunately, I will not be able to entertain anyone after Alan on this topic and I will make proposal. Alan, please go ahead.

ALAN GREENBERG: Thank you very much. Can you hear me now?

JANIS KARKLINS: Yes.

ALAN GREENBERG: Okay. As I started off saying, if had resolved the legal/natural person situation differently, this use case probably wouldn't exist. So that's an important factor.

Stephanie said ICANN doesn't look at data. We're not asking ICANN to look at data or how a website is used. Registrars on the other hand, are contractually required to consider use in some cases. What we're saying is the contracted party may look at the use and decide that this is indeed a valid access request for a legal person data and make that decision.

James's presumption is no consumer will ever be able to make a sufficient case that will convince a contracted party, and I believe that is not something we can say in the general case because it depends very much on the specifics of the individual situation. And as we have said from the beginning, this is a manual decision. This is not something that we're going to automate and therefore we believe it is a valid use case. It's a valid use case predicated by the fact that we currently do not have a legal/natural person distinction and there may well be cases where the controller looks at the situation presented and says it is a reasonable request. That's all we have said from day one. Thank you.

JANIS KARKLINS: Thank you very much, Alan, for this comment. I see that there is a rather big reservation from some groups on the case. There are groups speaking in favor. As suggested in the methodology, now it would be time for groups to provide inputs in writing in favor against and move the debate on Google Doc that I'm suggesting to do and maybe in two week's time, we can see what is the result. In any case, I think we have extracted a few grains of this conversation that will be reflected in the zero draft.

With this, I would like to draw the line under this agenda point. I would like to suggest to move to the last agenda item and that is on our next activity. I was told that we need to present a work plan of the team to the GNSO Council. In this respect, the suggestion is that next Tuesday on the 13th, for those team members who would be interested in listening to the proposed work plan, which would then submitted to GNSO Council. To do so, at the time our

call at 2:000 UTC. Also with understanding that Los Angeles meeting results may introduce significant changes in the work plan either to the positive side or to the negative side.

The next regular team meeting would be scheduled on August 15 as usual. So would this specific proposal to have a session on work plan would be acceptable. I see Berry would like to say something more than I do. Berry, please go ahead.

BERRY COBB: Thank you, Janis. Just to note that tomorrow morning you'll see in your inboxes the project management package for this particular EPDP Phase 2. If you'll recall, I did a brief presentation in Marrakech about that package. So there will be six or seven documents within there. Mostly Tuesday session will be focusing on the Gantt chart or the project plan which is the core of what will be carrying forward to the council, and just noting that we're attempting to try to get approval from the council on this preliminary plan so that we can move forward and asking for the final round of resources to support this group to the Board.

Again, over the weekend and Monday, review through these. I'm sure you'll have several questions or misunderstandings or difficult to understand about what's being contained in the project plan but we'll spend a fair amount of time on Tuesday going through that to help you understand what the tasks are in front of us which is ultimately the topics that we'll be needing to deliberate on, leading up into initial report and those kinds of things. Secondarily, these tasks have duration and dependencies assigned to them that

ultimately try to give us some clarity around the possible deliverable dates, but more on Tuesday. Thank you.

JANIS KARKLINS: Thank you, Berry. So that brings us to the end of the meeting. Thank you very much to all team members for active participation. This meeting stands adjourned. Have a good rest of the day.

TERRI AGNEW: Thank you, everyone. Once again, the meeting has been adjourned. Please remember to disconnect all remaining lines and have a wonderful rest of your day.

**[END OF TRANSCRIPTION]**