ICANN Transcription

EPDP on the Temporary Specification for gTLD Registration Data

Thursday 18, July 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/5HAkf2WpMDT7bWtnBxYuZyykv1hsrzrEdpvqz9LR8NHgp8RsEatSyuPXohDbjcym

Zoom Recording:
https://icann.zoom.us/recording/play/wndts9JfHtZT5gJLgBY2MNmbchfbr8wUs7fDVAHXBgC4dfXaG_axl1CjzUnlgvt9?startTime=1563458590000

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

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 18th of July, 2019, at 14:00 UTC.

In the interest of time, there'll be no roll call. Attendance will be taken by the Zoom room. If you're only on the telephone, could you please identify yourself now?

Hearing no one, we have listed apologies from Alex Deacon, IPC, James Bladed, RRSG, Volker Greimann, RRSG, and Farazaneh Badii, NCSG. They have formally assigned Jen Gore, Theo Geurts, Sarah Wyld, and David Cake as their alternates for this call and any remaining days of absence.

Alternates not replacing a member are required to rename their line by adding three "Z"s to the beginning of their names and adding, in parentheses at the end, their affiliation-dash-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 the chat, apart from private chat, or use any other Zoom room functionality, such as raising hands, agreeing or disagreeing. As a reminder, the alternate assignment for must be formalized by way of the Google assignment. The link is available in all meeting invite e-mails.

Statements of interest must be kept [updated]. If anyone has any updates to share, please raise your hand or speak up now.

KRISTINA ROSETTE: Hi, it's Kristina. I have a statement of interest update that I have not had a chance to put in yet. The folks in the CPH know this, but I have left Amazon, although I will continue to participate as an EPDP team member for the Registry Stakeholder Group until the stakeholder group has had an opportunity to identify a new member. Thanks.

TERRI AGNEW: Thank you, Kristina. Hearing no one further, if you do need assistance updating your statements of interest, please e-mail the GNSO Secretariat and we'll be able to help.

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.

Thank you. With this, we'll turn it back over to our Chair, Janis Karklins. Please begin.

JANIS KARKLINS: Thank you, Terri. Good afternoon, good morning, good evening, everyone. We are now starting our ninth meeting. We have an agenda that was circulated for your review. No comments have been received. May I take that as we would wish to follow the proposed agenda?

I see Milton's hand up. Milton, please go ahead.

MILTON MUELLER: I did comment on the agenda on the list, and I would propose that, instead of going through the use case ranking exercise, we would begin by discussing a possible consolidation of the use case into a smaller number of cases. I imagine most of you know the reason why I'm proposing that if I've not stated in clearly enough on the list. I think, before we rank, if indeed many of the cases are basically the same, we should group them and consolidate them before we rank.

JANIS KARKLINS: Thank you, Milton. Would you mind if we would take up your suggestions under Agenda Item 4? Even that is a use case ranking exercise, but this is related to ranking in this one.

MILTON MUELLER: Yes, that'd be fine.

JANIS KARKLINS: Thank you. So we will do so. Then, probably depending on the outcome of the discussion, we may not be able to get to Item 6, but again, we will see. I do not want to prejudge the outcome of the conversation on Agenda Item 4.

With this understanding, I would then go to the next agenda item. That is housekeeping issues. As you know, on Tuesday there was a meeting of the Legal Committee. I would like to see whether the facilitator of the committee, Leon, is on the call. I do not—

LEON SANCHEZ: I am, Janis.

JANIS KARKLINS: Okay. Leon, would you like to brief the team on how the meeting went and what are the next steps?

LEON SANCHEZ: Thank you very much, Janis. As Janis was mentioning, we held the first Legal Committee Phase 2 call. I think it was a fruitful call, even though we didn't actually get much substantive discussion on many questions. We were able to establish, of course, our working method. This will be pretty much the same as we did during Phase 1. We also went through some of the questions that

are pending in the pipeline to be answered by Byrd & Byrd – well, more that need to be answered by Byrd & Byrd – that need to be reviewed by the Legal Committee and then afterwards possibly submit it to Byrd & Byrd.

So we did this exercise. We realized that there are some questions that would be worth consolidating as they might be conflated/related issues, or they referred to the same issue in a different way. We began by tasking some of the members to consolidate some of these questions, and we will continue to analyze these questions to see which of them may be consolidated with others.

We will also begin doing an exercise of prioritizing the questions so that we, of course, focus on those that seem to be more relevant at this stage because we also realize that there was some questions that, at this point in time, it's not that they were not relevant but they were just too early in the process to actually be submitted to legal counsel. So we're going to be doing this exercise, too, of prioritizing and saying, "Okay. So is this a right question to be asked at this moment, or should we put it on hold until the right time comes?"

So this is pretty much what we spoke about, Janis, and I am of course happy to answer any questions.

JANIS KARKLINS: Thank you. I see Amr's hand up. Amr, please go ahead.

AMR ELSADR: Thanks, Janis. Thank you, Leon, for that briefing. It was really helpful. You touched upon what I wanted to ask shortly after I raised my hand. You mentioned the prioritization of questions because the responses to some questions might be more urgent depending on where we are in our workplan.

I was also wondering whether budgetary issues are concern at all. Are we going to be limited in the number of questions we can ask because of budgetary issues? And will this also require some form of prioritization of what questions we need to ask? Or is this not an issue that we need to factor in? Thank you.

LEON SANCHEZ: Thanks, Amr. Yes, budgetary issues were also mentioned. We have a limited budget, of course, at this point, which I understand is a preliminary budget that we established for the initial needs of legal support that the work will be needing. So of course this initial budget seems to be low to everyone, but I understand that this is also something that would be – once we know the real need for legal counsel by the group, then we would submit, of course, a request for additional budget. How this is going to work I am still not sure. This is something that of course the leadership team will be handling. But as far as I understand, this is just a preliminary budget.

Once we have identified a real need for legal advice, then we would be able to do an estimate of cost and submit that cost for consideration and hopefully approval. It may well come to the point in which we also need to prioritize questions in terms of

resource availability. So, yes, this is something that is also on our plate to discuss.

JANIS KARKLINS: Thank you, Leon. I see no further requests for the floor. Of course, it goes without saying that whatever outcome of the work of the Legal Committee that will be produced will be brought to the attention of the team a whole for endorsement.

Let us move then to the next item, and that is originally phrased as the use case ranking exercise. But as you know, Milton has made a proposal on the mailing list, and I will now invite Milton maybe to say a few words about it. After that, the team members can react in favor or opposition. Milton, please?

MILTON MUELLER: Thank you, Janis. We did send a document to the list with essentially … I'm trying to bring it up here.

JANIS KARKLINS: While we are looking, can I ask staff to put it on the screen, please? Thank you. Milton, go ahead.

MILTON MUELLER: A grouping was essentially – we felt that there's basically a fundamental distinction between criminal law enforcement and civil cases in which most of the key issues regarding policy would be the same. For example, if it is indeed criminal copyright violation of trademark or some kind of a botnet, the law

enforcement agency would be involved, and they would be requesting the information, whereas, in civil cases, it would be a non-state actor, a private party, who would be requesting the information. Again, it wouldn't matter a whole lot. I don't understand how it would matter whether this was copyright infringement, trademark infringement, consumer protection – those kind of things – fraud investigations.

We also proposed a grouping of what we call random forms of validation. Now, our opinion was that none of those cases should actually be considered. But whether you agree with that or not – I'm sure some of you don't – they all again share a distinctive pattern, which is that people are proposing to use WHOIS to do some kind of validation for their own private purposes and that, again, there would be a symmetry in the needs and demands, and the legal issues regarding a privacy law compliance would all be very similar in those cases.

Then the issue of contacting the registrant. Again, we saw three cases which really were proposing to do that. Again, we didn't particularly like those cases, but whether you agree with that or not, I think there is a symmetry in the motivation and type of request we're talking about so that, if we do end up going through those use cases, we would want to group them as essentially a single use case.

Then we had what we saw as standalone cases, which was the UDRP/URS request and the issue of maintaining a domain name registration by the registered name holder, which we saw as an interesting issue, a debatable issue – whether we need that use case – so we actually prioritized that. But again, for our purposes

now, we're just discussing whether it needs to be grouped with anything else, and we didn't think it did.

So those are the proposals that we made. Let the discussion begin.

JANIS KARKLINS: Thank you, Milton. The floor is open for comments. Actually, I would like to ask the team members to react very clearly to Milton's proposal of grouping use cases. Should we do it or shouldn't we do it? So should we do it, then of course ranking would come after the consolidation, but let's see what is the temperature in the room and what's the preference of the team.

I have a number of requests. Let me start with Hadia followed by Sarah. Hadia, please go ahead.

TERRI AGNEW: Hadia, it's Terri. If you're speaking, we're not hearing you.

JANIS KARKLINS: Hadia?

It seems that Hadia has technical issues. We'll come back to Hadia. Let me call now on Sarah, followed by Greg. Sarah, please?

SARAH WYLD: Thank you. Good morning. As I said in the chat – I see Milton is actually answering now as I speak, but I will still ask my question – we find that there is value in working through a single specific use case from start to finish. If they are grouped in this way, how would we do that? Would we look at one of the use cases in each group as exemplary? Or what would that look like? Thank you.

JANIS KARKLINS: Thank you, Sarah. I think Milton responded. The idea is maybe to make those cases more general and then look to all aspects in a more holistic manner. So that's, I understand, the idea. But it would be also interesting to see whether you think that would be useful or not.

Greg?

GREG: Thank you. We should definitely group them together. There are a lot of cases that have a lot of commonalities with each other, and maybe a case of finding the one that's most exemplary, walking through it very carefully, and then seeing where additional ones diverge of add some detail. But are there definitely some time-savings that can be had.

Regarding the document on screen, the header – Criminal Law Enforcement – is perhaps not the best one. Law enforcement is different than private parties who deal with crime. The group one might just be called Crime, actually. The list is also missing two of the three SSAC cases, so we want to make sure that those are included.

So there's some work that somebody can do to find the best cases within each category. We should probably concentrate on those and then add in detail from others. But we can spend a lot of time otherwise, and I think we can whittle this down a lot. Thank you.

JANIS KARKLINS: Thank you, Greg. If the team would be favor of Milton's proposal, in that case, I think the most valuable way forward would be to ask the Secretariat with the help of some volunteers to make a first stab and then make it back to the team for consideration.

I see next is Chris Lewis-Evans.

CHRIS LEWIS-EVANS: Thanks, Janis. I'd just like to thank NCSG and Milton for this good grouping. They've obviously spent a long time considering where it goes, and it's quite well-done, to be honest. Obviously it's fairly late – I think it was yesterday – that it came out, so I've not managed to go through how every single case fits exactly in with that. I quite like how it's done and agree that the grouping is definitely beneficial and [inaudible] having gone through it with a fine-tooth comb, I certainly agree with 90% of where it is and agree with your recommendation, Janis, of just doing that and making sure we are happy as a group about the grouping.

I think we do need to be careful that we don't miss out things. So my initial thought on this is something like a cert or a national cert is missing from this grouping because it wouldn't really fall in any of the groups here. But I think I've certainly seen a user case

where that's definitely a good requirement for us to [inaudible]. So I think I certainly support this way forward, but we just need to make sure we cover everything in the course.

Personally here I would prefer to pick one of the cases from the list rather than rely on the consolidated description that's being picked here. I think, for more, the consolidated description is a little bit broad and is more towards a purpose, rather than a user case. But that's my view on that. Thank you.

JANIS KARKLINS: Thank you, Chris. Greg, if you could your hand down. Let me see. Is Hadia available now?

Hadia?

HADIA ELMINIAWI: Can you hear me?

JANIS KARKLINS: If you could speak slightly louder, then we'll hear you well. Otherwise, we hear you but not overly well.

HADIA ELMINIAWI: Okay, great. Thank you so much. What I want to say is that actually, for the ALAC, we don't agree with the categorization that Milton suggested. For example, with the ALAC's two consumer protection organization use cases, some of the consumer protection organizations might be associated with government law

enforcement agencies, but this is not a requirement. You have also independent consumer organizations that work on protecting users online and preventing fraud.

With regard to the second ALAC use case, which is Internet users validating domain names, this is not about a curious Internet user. This is also for the public good because, if Internet users do not have a way or means through which, if they are suspicious and they want to check the domain name, to be able to do so. And if they suspect it after the data is disclosed, they can report it. This is an essential use case because part of preventing fraud is through consumers and not necessarily victims reporting websites and reporting domain names before the incident itself happens.

You have also the Organization for Economic Cooperation and Development, which had a policy paper on WHOIS that stated that an easy identification of online business is a key element for building consumer trust in the electronic marketplace. The OECD paper represents an international consensus about the importance of registration data for consumers. This is a policy paper that is actually available online.

So, in short, we don't actually agree with this way of categorization. Thank you.

JANIS KARKLINS: Thank you, Hadia. Next is Margie, followed by Brian.

MARGIE MILAM: Hi. I don't agree with this approach. I thought the staff breakdown on the wiki made a lot more sense. Given that we'd already [inaudible] to the exercise of prioritizing and things, I feel like we're going backwards to reshuffle the use cases at this point. It seems like we should just start through the process that staff identified on the wiki and see where the commonalities lie.

In particular, there's specifics within each of the groups that Milton has that just don't make sense to me. We can go through those separately if you want, but I think it makes more time for us just to go back to what the staff suggested. Thank you.

JANIS KARKLINS: Thank you, Margie. Brian King?

BRIAN KING: Thanks, Janis. I also agree with Margie. I prefer the staff's categorization. A couple points. I'd still like to be clear about what we're trying to achieve with grouping use cases. It seems like specificity is important, so I want to be clear with what efficiencies by doing this. I don't think we can assume that they're all going to be the same in any given use case. Sorry if I'm being thick-headed here, but I'm not clear on what exactly it does for us if we need to be specific about a use case and then drive forward from there.

Also, we obviously disagree with the document on the screen to the extent that there's no value or that these should not be considered all in Grouping 3 and 4. We think there is value in these use cases, so we would disagree with that. Thanks.

JANIS KARKLINS: Thank you, Brian. As you see, Milton commented that we have now 19 cases to examine. We have nine meetings to go until the face-to-face meeting and then another probably dozen until the November meeting. Let's assume we take one take per week. That means we will examine all of them only by ICANN 66. Then we will not have time to consolidate and discuss potential commonalities that would come up. So the challenge is that we have too many cases for the moment than time or weeks we have until the ICANN 66 meeting.

That said, some cases do have some commonalities. They're similar by nature. They have differences in some aspects. If cases would be clustered, then those aspects would be specifically taken out and then presented, but the overall frame of the case would be the same. So I think, if we go the way of grouping cases, then every specific aspect would be taken out, would be put in that consolidated case, and would be discussed by the team as we progress with the work. Again, this is, of course, your decision.

I will call now on Alan Greenberg, followed by Kristina.

ALAN GREENBERG: Thank you very much. I agree with the concept of grouping because spending time on evaluating the use cases that are very similar, I think, is a waste of time. I don't necessarily agree with Milton's specific grouping, but I do think it's important to group them together and not redo ones that are very similar. I don't think it's worth spending the effort trying to capture all of the concepts

from the various different ones into a single use case. I think that will end up being a rather confusing use case, difficult to handle, and I'm not sure of the merits of spending of the time on it.

But in terms of where we put our focus, I definitely think it's worthwhile identifying the generic types and pick one of each at least to do on a first-come basis and then see where we are once we've already done one of each type.

I'm not going to elaborate a lot more. I think that's where we stand. Thank you.

JANIS KARKLINS: Thank you, Alan. Kristina, please?

KRISTINA ROSETTE: Thanks. I do think that the concept of grouping can introduce some efficiencies if we are thoughtful about it. I would say that the primary concern that I would have that this point with regard to the grouping that Milton proposes is I do think it's important that we separate out LEA from the other quasi-criminal use cases that have been identified here. I do think that LEA is different. It has a different status there, different needs. Quite frankly, I think there is some value independent of that from being able to say, truthfully, that the first use cases that the EPDP completed were the LEA ones. I think that will be helpful throughout the community and for some of those actors outside the community that are watching the work and the pace at which we are doing it, as was alluded to in Marrakech. Thanks.

JANIS KARKLINS: Thank you very much. Next is Leon.

LEON SANCHEZ: Thank you very much, Janis. Can you hear me?

JANIS KARKLINS: Yes. Please.

LEON SANCHEZ: Thank you. I see a benefit in trying to consolidate use cases. As I was saying or suggesting back in Marrakech, I suggested that we focus on principles rather than single-use cases. I think that grouping these cases or consolidating cases will lead us into that because we will be able to identify the commonalities to which I refer by principles maybe. This would help the group to focus its work in less volume and more in, as I said or as I referred to them, principles that might be used across different cases.

I see also the challenge of singling out some cases that might actually have some particularities that need to be addressed, but then, as you suggested, I think that the mere exercise of trying to consolidate the cases will have us go through each and all of the cases. Then we will be able to do this consolidation if it actually works because one thing that I suggest is that we don't go into this exercise pre-judging that some case will actually be consolidated with another. Or we might come to the conclusion that consolidation is actually not possible.

So I would encourage us to go through this exercise of analyzing whether cases can be consolidated. If it's not possible in the end, we'll find out that we will already have grounds and a basis to actually say, "Well, if this didn't work, let's continue our work." We will already be halfway there when we realize that, I guess.

JANIS KARKLINS: Thank you, Leon. If I may, Milton, I will leave you until the end. I will first take Mark Svancarek, and then you, Milton.

MARK SVANCAREK: Thanks. Like so many other people, I do agree that we're going to wind up grouping a bunch of these things together. At least from the BC side, we just perceive that, if we created a bunch of more granular ones, they could be more easily combined later once analyzed, as opposed to trying to break out new ones if we found that things needed to be distinguished later. So it's always been in our mind that some of these things were going to be consolidated at some level, but how that process would proceed was unknown to us, and hence the conversation we're having right now. Certainly, we're open to some sort of consolidation, but doing it upfront? The more we talk about it, the more I think that doing it upfront is going to result in a loss of fidelity. And we're going to be missing out on a lot of good conversations that we're going to have.

There's at least three groupings I've seen now: the one that org has done, the one that Milton proposed, and there's a pseudo-grouping in the prioritization document that the BC sent the other

day. It's probably not obvious when you look at it, but that was actually created in a way to encourage grouping and consolidation going forward.

Given that there's competing groupings put forward right now, I would suggest that we start with the one put forward by org. Thanks.

JANIS KARKLINS: Thank you, Mark. And now Milton.

MILTON MUELLER: I think, based on what I've heard, I've heard a lot of support for the idea of grouping. I think the one issue that we also still seem to agree on is that we need to separate out the LEA cases and prioritize them. When I separated this criminal law enforcement from the other cases, this was essentially using the same rationale that Kristina and Alan Woods and others had been talking about, either on the chat or when they're speaking, that the state actor is a distinctively different kind of actor. The balancing test would be more tilted in their favor. I think that there would be a lot of commonalities if we're talking literally about law enforcement between any case construction.

I think that the problem with some of the cases that I've tried to group under that heading is that, when, let's say, the IPC talks about criminal copyright infringement, yes, they may doing some kinds of investigations to point law enforcement at a criminal case, but at the point at which the law enforcement agencies actually take action, you're basically doing a law enforcement action. I

don't really see it as a separate use case, whether it's trademark or copyright or phishing of a botnet. If a law enforcement agency is involved, it's a distinctive kind of case and there's a distinctive set of equities that we'll need to take into account.

Combating crime is a much too broad – that could actually apply to almost any activity that security people do, so I really want to keep that grouping much more specifically focused on law enforcement by government agencies.

I'd also like to express agreement with Kristina's point about, in terms of the people watching us and looking at our progress, that, if we can make progress on the LEA case right off the bat, I think that would be optically important. I really think that we could certainly agree on that much at this stage.

In terms of how then other groupings work out, again I see very little difference in the types of safeguards, the types of request for information, in the other groups, in particular what I call civil – maybe I shouldn't call it civil law enforcement. Maybe I should call it civil claims or private actor claims.

Again, I think if it's a consumer concern about fraud or IPC copyright/trademark infringement, I think we've already started working through that with Thomas Rickert's case. I think, as a general procedure, we could just take one of those cases as is for each group and then we could discuss later whether any of the other specific use cases add anything to it. I think that would be a good procedure for going forward.

JANIS KARKLINS: Thank you. I have a number of further request, but please – now it's the second round – if you could keep your comments as brief as possible. Alan Greenberg, Greg, and then Brian.

ALAN GREENBERG: Thank you very much. Milton's last sentence was exactly what I was proposing. That is, we need a grouping and then to take one and then see if there's anything else missing that really is important to consider.

I realized, as people have been talking, that Milton's Group #2 – civil law enforcement – can be multiple ways. Is it the enforcement of civil law, or is it quasi-law enforcement by civil entities? Certainly, in the way it's grouping it, it sounds like it's the latter, not the former. So I think, if nothing else, the titles of the groups needs to be really clear. What Milton has called civil law enforcement really is closer to fraud and related things that are performed by civil entities So I think we need to be careful on how we do the grouping and make sure that they are similar and not just law enforcement – legal law enforcement in this particular case. But I support that overall methodology. Thank you.

JANIS KARKLINS: Thank you, Alan. Greg?

GREG: I'll second what Alan says. We need to make a distinction between who is making the request versus what they are doing with the data and why they're requesting the data. For example,

the investigative techniques that law enforcement uses are in many cases exactly the same as would be used by a private party who, for example, is investigating a phishing case. Law enforcement has a particular status as an official entity, and they have maybe some different bases for making the request. But why they're getting the data and what they're doing with it may be the same as other parties. We'll see these cases come up, so let's also keep those two distinctions clear. Thank you.

JANIS KARKLINS: Thank you, Greg. Brian?

BRIAN KING: Sure, I can help, I think, directly address Alan Greenberg's question and some of the confusion here about law enforcement. I think the value – I'll answer my own early question – in grouping these use cases is that we can find commonalities in the purpose. What we're looking here is the third-party purpose and why the data should be transferred to that third party. The purpose of processing that data is to investigate or look further into or contact someone about a crime versus to contact someone about some civil wrong, some private harm. So I think that's the difference in the purpose. If we stay in that realm and not whether you have a badge and a gun or not and not whether you work at a police station or not, it's about the purpose and what you're investigating on any given website or any given domain name. So I think we retain the value of doing the groupings if we keep it focused on the purposes and not user groups and not all those other things that distracted us in the past. Thank you.

JANIS KARKLINS: Thank you. Alan Woods is the last one.

ALAN WOODS: Thank you. I just want to follow-up there very quickly on what Brian just said there. I don't necessarily disagree with what you said there, Brian, but at the same time, I think there is a huge difference when we're weighing the balance between a person who is doing investigations which happen to be of a criminal act as opposed to those doing investigations who can call it a criminal act or not or bring the legal process to it. I still think there is a subtle difference between those parties, and that will have a material effect at the end of a review of whether or not data is to be released or not. Again, yeah, having the badge and having the gun, as you said, does actually make a difference, say, if it wasn't a 61F consideration at the end of the day, as opposed to a company who's trying to do brand protection, for example, through criminal [acts].

So I just think we need to be careful that we're not lumping genuine law enforcement with people who are trying to help law enforcement. It's slightly different.

JANIS KARKLINS: Thank you. I think we already in discussing how the grouping should be organized. Probably we do not have enough time to do it here during the plenary meeting.

If I may suggest the following way forward, it seems, of course as usual, we have differences of opinion, but I have a feeling that we may try to do some kind of grouping, not necessarily according to Milton's proposed four groups, but to look at maybe also what staff proposed. If you would agree, I would ask staff to do the first cut maybe with the help of a few volunteers from the team.

I think Milton would be a very natural volunteer in this case with maybe somebody from the BC or from the IPC who could join and do this grouping proposal and bring it to the attention of the team maybe next week, if that would be possible or, in the worst case, the week after.

In the meantime, we would continue working on open cases that we have started examinations [on], specifically on law enforcement. Then, if we finish with the current law enforcement, we may take a next one until we agree on possible groupings and examination.

I think one thing that came out from this discussion that is important is that, even if we examine one case, we may bring to the attention of the group elements which are different from similar cases and go through them on the basis of the case which we're examining. So if that would be acceptable first and foremost for the staff, Marika, would you take up this duty?

MARIKA KONINGS: Thanks. Just to note that staff already did take a first cut. I think that's what's on the wiki, where we did already try to organize or group certain uses together under a certain heading. We can, of

course, take indeed what Milton has done, as well as the input that the BC and IPC provided in response to the survey and try to compare and contrast, but it would be really helpful if people could provide more specific – for example, if Milton could provide specific input on what he didn't like about the staff grouping. I think several people have already made suggestions on – and Milton's grouping might to be different. And if people can also look at the BC and IPC suggestions and indicate what they may not like about that. Based on that, we may then be able to come up with some of new organization. But as I think you indicated and several have suggested, the grouping doesn't mean that anything is going to be left behind. I think we're looking for the best way in grouping the uses cases by having the most representative case discussed and still being able to look at other use cases if there is something that is significantly different that would resolve different responses to the template questions.

In short, staff is happy to take this forward, but it would really helpful to get a little bit more input on what people didn't like in the original grouping, as well as the other groupings that have been suggested so we can use that in creating a hopefully acceptable grouping [poll].

JANIS KARKLINS: Thank you. I was expecting you to take up this task. Thank you very much.

On volunteers, Milton, you will volunteer, right?

MILTON MUELLER: Yes.

JANIS KARKLINS: Thank you. Then others. Brian?

So please think not – yes. Thank you, Brian. Who else wants to volunteer, with the understanding that we would get a list for next Thursday to examine?

Thank you. So then we have agreement on the way forward. Thank you. And Marika will organize a small list for volunteers. Thanks.

Let us now move then to the next agenda item, and that is the user case investigation of criminal activity against the victim of jurisdiction and investigation of E.U. law enforcement requesting data from non-local data controllers. Can we get the case on the screen? Yes, there.

What I would like to propose as a methodology is the following. We maybe ask Chris Lewis-Evans very briefly to walk us through the changes introduced, and then we will go chapter by chapter and see how far we can get in the document in agreeing in broad lines on that. Chris?

CHRIS LEWIS-EVANS: Thank you, Janis. If we can scroll to the safeguards because realistically that is the part that has had the major changes, as per last week's call, what we discussed was trying to separate these out into manual and automatic processes and then also flesh out

other bits and pieces that we could add. Myself and [Georgios] worked on this to try and add some extra bits and had taken on some of the comments, I think, from Thomas's example. We've added some parts where only the data requested and the data that is necessary is supplied. So it depended on whether you are the requester of the disclosure where we view the word "necessary" on there.

The second point there is a little bit of a holdover. When we get to automatic, it's expanded a little bit better. Really what that is is a place marker for applying to [look at] the norms of data protection – holding your data encrypted [at rest], making sure it's all handled appropriately and you're not or you are destroying it after use and everything else like that. So that's more of a [inaudible] caption there. If we can scroll down a little bit more … a bit more because it's a big change. Just after [inaudible] requests. Thank you. Obviously, this one is for a manual process. We've got there that the disclosing parts must define and perform a [balancing] test, which is obviously a big part of that.

The second part is, because this is a law enforcement use case, we said that the system must allow for some consent/confidentiality whilst the investigation is ongoing.

So those are the two main parts there. Two parts are to do with automatic systems. You can scroll down again, please. This is obviously mainly new, which is why there are lots of changes there. Very similar to manual. It becomes a little bit more specific there with what the requester must do with the data they receive: store, protect, and expose the data in accordance with relevant data protection laws.

Also, as it is an automatic section, we've got the part where they may be subject to the accreditation and be reported to a relevant DPA if they are found to abuse the system at all or the data that they have been given.

If we scroll down, we get onto disclosing the system. Sorry, it's always a pain [inaudible]. Again, only supply the necessary data, which we've covered quite a bit, and it's the right thing to do. Current data sets and no historic data is [inaudible]. Further down, we talked about must have a monitoring system and then allow them to do auditing. So if there is any requests around how the data has been used, that can be properly fulfilled. Monitor and log. So that goes against high-volume requests. Whenever you're doing proper monitoring, you can see abuse of the system via whether it's mass requests or whatever. Then, again, a form of disclosure to the data subject upon request with, again, that confidentiality.

The next sections are all pretty much the same. We can go onto the accreditation and what would be required for the information to be released.

So I think that's a very quick overview of what's changed.

JANIS KARKLINS: Thank you very much, Chris. Let me then propose to let us go to the very beginning, and we will walk section by section and see whether we can get broad agreement on everything that we have in the case. If you please consider this as a final reading of these sections, we would not come back anymore to them, specifically

as a reading of the case. If need be, we will revisit when we will discuss commonalities, if we will need to go back just to re-discuss something on substance.

The overarching purpose. Any specific comments on the overarching purpose? Milton?

MILTON MUELLER: I did present an objection to a large part of the second half of that overarching purpose. I thought that it was extremely broad and capable of justifying almost anything: public health, any vital interest, threats to the governments – its people, property, interests. Again, I think that's not a use case. That's a very, very broad level of authority. I don't see why you need it to develop this use case. I think everything that you need is covered by a government authority to investigate, detect, prevent, disrupt, and prosecute criminal activity, including but not limited to terrorism. Period.

We know that national security in particular provides a very broad exemption from all kinds of things, including tariffs on steel exports, apparently, from Europe. I'm just uncomfortable with that broad of a purpose.

JANIS KARKLINS: Thank you. Brian? Your reaction?

BRIAN KING: Thank you. I think this is good. I think it's good to be specific and detailed here. I like that we have all this language, and I definitely support this one. I think it's going to be good to show our homework and specifics. I think, in general with these use cases, broad is good. We'll get legal advice and we'll find out if these are going to be legal or more specific. I'm not worried about being overreaching at this point. In fact, I think the exercise does need to be very broad here so we can capture, in an automated fashion, as much as this possible, and, again, with legal advice to say that that's fine, which we'll ultimately get or not. But I would say that it's better now to be broad, and I like that this is sufficiently encompassing and specific. Thanks.

JANIS KARKLINS: Thank you. I have Ashely now on the line, Ashley, please.

ASHELY HEINEMAN: Hi. Ashely with the GAC. I just wanted to, I think, echo something I had already mentioned earlier, which is that I'm concerned that activities such as those associated with certs are [logged]. What was good about Chris's full text is that it would fall under here. I'm not opposed to modifying it in a way that perhaps limits it a bit more, but I think, with the edits that Milton provided earlier, it was too much. I think the primary issue here is, at least in this very specific case of government certs, is that they're not sworn law enforcement. That's how we make the distinction a lot of times. For example, it's a lot easier to accredit law enforcement is you're sworn law enforcement. So it's examples like this which is why I think it's important to keep this text broader. But again, that being

said, I'm happy to consider ways to truncate if there's agreement that Milton's concerns are warranted here. Thanks.

JANIS KARKLINS: Thank you. Chris Lewis-Evans?

CHRIS LEWIS-EVANS: Thank, Janis. Do you want to let Margie go first? Then maybe I can [inaudible] the point at the end. Thanks.

JANIS KARKLINS: Okay Margie, please?

MARGIE MILAM: I think the purpose and the whole thing makes a lot of sense. Milton's approach, I think, narrows is far too much, so I would propose keeping the purpose close to what is listed here a lot and try to get legal input to see if it works. Thank you.

JANIS KARKLINS: Thank you. I see now David. Let me take – Chris, I will put you at the end of the line if you don't mind. David Cake?

DAVID CAKE: Hi. Speaking to this preamble, are we distinguishing here between government authority to investigate criminal activity or just government authority to investigate [inaudible]? I'm thinking of issues here like, for example, public health, where the government

statutory bodies may have authority to investigate but it's [not] without an indication of criminal activity. Are we try to include general government ability [for] statutory [investigation] in this without – or only looking at criminal issues? Thank you.

JANIS KARKLINS: Thank you. Chris?

Chris?

CHRIS LEWIS-EVANS: Sorry. I was still on mute. Thank you. On this purpose, I've actually gone to one of our governmental DPOs and had them take a view on this. They are happy with the language and confirm that they think it's a valid purpose of the GDPR.

However, certainly from Milton's point, I think what we need to be a little bit aware of in this group is that obviously that is framed by our legislation and how that works. That may be different country to country and could cause some issues. So certainly I can have a look at this to see if maybe we can make it a little bit narrower to answer some of Milton's points.

David has just raised a really good point there. I think maybe another way of framing it is what the public healths are able to do. If that is to investigate a criminal thing for public health, then that is one thing, but, obviously, to prosecute is completely different. I can think of a couple ways forward, and certainly, from what David has just said, maybe I also want to [inaudible] Milton's concerns. So maybe it's an action for me to go back to our DPO and see if

we can frame it slightly differently to maybe answer some of those.

JANIS KARKLINS: Thank you. I think that there is a very good justification to speak about law enforcement in the context of protection of national security and national safety. Maybe public health falls out from that logic in the first look. Maybe I do not understand some concept behind that specifically mentioning public health. But then the rest of vital interests – national persons and the governments' protection, threats to government, threats to people, property, interests – all falls within the authority of law enforcement.

Let me see now. David, is this a new hand or an old hand? Otherwise, Mark. David?

DAVID CAKE: Sorry. Old hand.

JANIS KARKLINS: Mark, please.

MARK SVANCAREK: As we go through this exercise, I think this is a great opportunity for us to think about how we're going to do grouping and consolidation. We had one set of feedback that said perhaps this is too broad. Then we had counter-feedback that said this specific suggested narrowing leaves out cert, for instance. So how would you capture that conflicting feedback in a single document as we

go through the process of consolidating and grouping? Would you start with the narrower case and then say, “Plus here’s some possible expansions which might be their own use cases,” parenthetically like that? Or would you start with the bigger case and say, “Here are some narrower cases that fit underneath this one”?

I’m not saying that I have the correct answer today, but I think that, as we go through this exercise, we should not be putting off the thought exercise that needs to happen later. How exactly do we go from this list, however big this list is, to do the grouping as a practical exercise? I’ll continue to think on that and make suggestions if I come up with anything, but really I’m calling on everybody to keep that in their mind as we go through this exercise. So as we’re going through this very specific one, think about the other ones or other ones that have been mentioned and stuff like that and how, if they were narrowed, you would represent that here. How, if they were combined, would you represent that there in this template? Thank you.

JANIS KARKLINS: Thank you, Mark. If there will be a merging common understanding, we will use that and capture that for the document. For the moment, the policy proposal is not written and will not be written until we will have some substantive material to put in it. I think the conversation gives a certain sentiment that we will need to remember in order to translate that sentiment in the final document. I think that staff is well-placed for doing that and capturing those elements, even if we disagree with each other. I think, for agreement, what we have at the moment is that law

enforcement agencies or agents have uncontested rights for doing their job in [inaudible] exercise. So there's no questioning there on their rights of doing these things.

I understand that Mark – sorry, Lewis-Evans. Chris – my apologies – will go to their law enforcement experts and will try to fine-tune that overarching purpose in light of conversation and will propose any modifications in the final version that will be published for our benefit.

Can we move to Use Case Sub-Item A? Any objections/comments? Marc Anderson?

MARC ANDERSON: Can you hear me okay?

JANIS KARKLINS: Yes, Marc.

MARC ANDERSON: I guess I want to react to what Mark Sv said because I think he made a point that really got me thinking. It's awful hard for us to go through these use cases line by line when some people are looking at each of these lines in terms of, "Should this be a specific narrow representative use case?" and some people are looking at them as "Should this be a broad, general, generic use case?" I think, when we went through the first line, we had some people making conflicting statements, but depending on the path we take, their statements might have been incorrect or might have

been off-track. So I think it's going to be hard for us to go through line-by-line until we agree on if this should be a generic, broad use case or should this be a specific and narrowly-focused use case. I think that's going to make it challenging for us.

Second point. On the use case language itself, first I want to thank Chris and everybody that worked on this use case. I've had the chance to look through it in detail. One thing that really struck me about this particular use case is we're talking about investigation of criminal activity when you're requesting data from a non-local data controller. The key to this one is what I understand to be is where the action is cross-jurisdiction or outside of jurisdiction, which I think is a complicating factor for us and something we maybe haven't spent enough time talking about.

You have three actors, or maybe four in this case. You have a victim that's in the jurisdiction of the investigating law enforcement agent who's requesting data from a non-local data controller. The controller is in a different jurisdiction, and presumably, I guess, we don't know the jurisdiction of the data subject at this time in the use case. But we've got three or four areas where we're potentially crossing jurisdictions. For me, that's one of the key aspects of this use case: revealing this cross-jurisdictional transfer of data, where we have potentially three or four different jurisdictions to consider. Maybe that's something that needs to be spelled out a little clearer in this particular use case.

JANIS KARKLINS: Thank you, Marc. Look, if I understand correctly why we're doing this exercise, it's not to fine-tune this use case to perfection but

rather to capture and grasp issues that require our attention. We will then put those issues, if appropriate, to the policy recommendations, and then we'll see whether we can agree in what or how we need to rephrase those recommendations that we are all on the same page on.

For instance, if we take the overarching purpose, then probably that will be a general statement of the purpose of law enforcement requesting data disclosure. That might be if we will come to agreement. That might be broad enough – the captures, every aspect – because, in the policy recommendations, most likely we will not be able to take up every specific situation that may occur in a real-life situation. We're just using these cases as examples to fine-tune our thinking and our common understanding and start with capturing these things. We'll try to transfer that in the policy recommendations. Then we'll be presenting them as a zero draft to the team to see whether it has been a successful exercise or not. Then we will go through these policy recommendations and we'll try to reach consensus or agreement on those, but not on every single line in these use cases. At least this is how I see the exercise that we are going through now.

Hadia, you are asking for the floor.

Hadia, your hand is up. Please go ahead.

HADIA ELMINIAWI: I am speaking.

JANIS KARKLINS: Hadia?

HADIA ELMINIAWI: Yes. Speaking.

JANIS KARKLINS: Yes. Please go ahead.

HADIA ELMINIAWI: I have a quick comment with regard to our discussion about how broad the use case is or not. I would like to refer to the Budapest convention on cybercrime, which is an international treaty on crimes committed via the Internet and other computer networks. It deals with infringements of copyright, computer-related fraud, child pornography, hate crimes, and violation of network security. All of that is mentioned in the Budapest convention.

I don't think the use case that we have here is very broad. Again, I'm saying that because I [learned] at the international Budapest convention that it covers even more than that. Again, we could think about limiting the use case, but then again, how useful would that be? Thank you.

JANIS KARKLINS: Thank you, Hadia. Again, I can only repeat that, or me, we're using these use cases to align our understanding of these things. Then we could try to translate [them into] the policy recommendations.

Shall we go back to small "a"? Any comments on user groups/requesters?

No? Then small "b": why the non-public registration data is necessary. Any comments on this part?

I see Milton. Milton, please go ahead.

MILTON MUELLER: Just a question on why this only refers to the secondary victim and not to identification of the criminal or to the primary victim.

JANIS KARKLINS: Thank you. Let me take Marc Anderson before Chris. Marc, please?

MARC ANDERSON: Thanks. I have to say that the explanation in "b" for why non-public registration data is necessary doesn't really seem to align with the purpose at the top. So I guess that's a question for Chris. This "why it's necessary" is very narrow, which doesn't seem to align with the purpose. So I guess that's a question for Chris.

JANIS KARKLINS: Thank you. May I call on Alan Woods now?

ALAN WOODS: Thank you. I suppose my question goes a little bit deeper. I think potentially the whole concept of necessity here is actually not – I

think we've missed the point somewhat because that's not answering the question of why is it necessary. The question on necessity is, why is this data from the contracted parties, for instance, necessary to achieve the purpose? This doesn't answer that at all. It doesn't say, is it the only source? Are there any other ways in which law enforcement can get this data? Are we a last resort? Is it necessary, given the effect of the investigation? I don't think he's thinking of necessity in the correct way here, so I would suggest having to change that.

JANIS KARKLINS: Alan, if I understand, you're proposing to change what is on the left-hand side – why is public registration data is not necessary – not what is one the right-hand side (the answer). Right?

ALAN WOODS: No. Sorry. I think the concept of necessity under the GDPR specifically is not about giving a reason why you need the data. It's giving a specific reason of why you need the data in this instance from this people, and what have you done prior to getting this data? So it's [inaudible] an explanation.

JANIS KARKLINS: Okay. I understand. Thank you. Actually, when I made my private consultations with the different groups here present on the team, I was told that, in reality, the personal data can be gathered in a different way. Simply, the WHOIS database is the simplest and the shortest way of getting to that data and also the fastest way. Again, I just [relay] what I understood from conversations. We're

here simply balancing those different aspects. But I may be wrong. Let me ask Chris.

CHRIS LEWIS-EVANS: No, I think you're right there, but to go to Alan Woods's question, yeah, I didn't answer it in a necessity-type way, just why it – I almost took the question literally, I suppose, and said, "Why is it necessary?" Then, to go to Marc's question about does it align and is it maybe to narrow, I think I was trying to be a bit more specific about why we would [inaudible] maybe because I had necessity in the back of my mind and I was answering that. [inaudible] going to Alan Woods, if we want to change a question to go more along [inaudible]. Now I'm going to give up on that word. If we want to go down more to what Alan Woods was saying, then we can certainly reword that and get that out. That should be fairly easy to do.

JANIS KARKLINS: The question of Milton was, why only the secondary victim? Not the primary victim.

CHRIS LEWIS-EVANS: Because, for the primary victim, we wouldn't have to go to the controller to get the WHOIS data because we would be conversing with the victim.

JANIS KARKLINS: Okay. Thank you. Alan Wood, is that an old hand? New hand?

ALAN WOODS: It's a new hand.

JANIS KARKLINS: Please.

ALAN WOODS: Just very quickly. Chris, yes, absolutely. The reason why I think we should interpret it as the other form of necessity is that that is what is expected under the GDPR and that is, I suppose, is one of our guiding principles in this, so we should do it that way.

Janis, to respond to your point, what you're saying is right. Please do get me wrong in the sense I'm saying everything must be absolutely necessary because this is one of those [track horses] of the work that we've done. I'm not saying it has to be absolutely necessary. It just needs to be reasonable necessary. I see Milton is talking subpoenas and it has already started a conversation of, why is a subpoena necessary? No. it needs to be justifiable and reasonable that, in this instance, the data is reasonably necessary in order to support this and there isn't another more direct or legal manner of doing this.

I just want caution us on this concept of that something is easy or something is not easy. That is not a good enough reason to be necessary. WHOIS for many years was considered to be the easiest way. However, we know that know that WHOIS for year was not necessarily the most legal of ways. But it was easy,

absolutely. But it was not legal. So we just need to be very clear that ease does not equal necessity.

JANIS KARKLINS: I think that this part of conversation reveals that there might be something to capture for the policy recommendations in relation to that ease of access to information does not necessarily mean that the access will be granted, provided that there are some other ways of getting that and so on. This is why we're talking through these cases: that gives us some interesting thoughts that may be captured in the policy discussion.

Chris, based on this, would you think that the part in small "b" should be amended in any way?

CHRIS LEWIS-EVANS: Yeah, definitely. I think we can [inaudible] from necessity and maybe just, as Alan Woods just said there, change the question to "What is public registration justifiable and necessary?" or "justifiable and" – I forget what the word was he used. That might bring out better answers for future templates as well.

JANIS KARKLINS: Okay. Thank you very much. Any other comments on this part; small "b"?

Alan Greenberg?

ALAN GREENBERG: Just a very quick one. Ease is not an issue, but ease may well correspond to practicality. The ones that are not easy may in fact be so difficult that they are not practical at all. Therefore, "ease" certainly is the wrong word, but there may a corresponding other set of words that are reasonable in this case. Thank you.

JANIS KARKLINS: Thank you, Alan. Let us move now to small "c". Any comments on small "c"?

Milton?

MILTON MUELLER: It looks like, although it's hard for me to keep an eye on this moving target here, the data elements – many of them – are in public WHOIS. I just wondered whether basically they just copied and pasted all the data elements because any one of them might be needed. But I would have thought that this would at least be limited to redacted data elements that would be necessary.

JANIS KARKLINS: Thank you. Any other comments before Chris responds?

Chris, please.

CHRIS LEWIS-EVANS: Thanks. Yes, Milton, I did put everything in. If we can scroll to the right, at the bottom I put a reason why. We need to make certain that we're processing the current data. When a request goes in for

the data, what you want to be doing is getting it from a single known source, rather than maybe having to query two separate sources. At the end of the day, we're going to the de facto place for getting this information. There are large implications for processing this data to the data subject if we get it wrong. Therefore, I think it is practical and necessary for us to ensure that we're carrying out processing on the correct and [current] information. That's why I put down everything there.

JANIS KARKLINS: Thank you, Chris. Milton, you're satisfied? Marc Anderson, please?

MARC ANDERSON: Thanks, Janis. Just a clarifying question for Chris. I understand your explanation for why you would want redacted and public. I'm wondering. In this use case, would you be requesting all data every time? Or is this just the entire set of data that you might ask for, and in the request you envision specifying which data you need in this particular request and [inaudible]? I guess that wasn't completely clear to me. So I guess that's a follow-up for you there.

CHRIS LEWIS-EVANS: I think we maybe did this face-to-face with a couple people but maybe not in the whole group. No, I think for this user case, depending on the actual crime committed, you may require every single piece of that data there. But for others, you may only require a subset of the information. Again, that is down to a case-

by-case necessity for that information. But on any one case, you may require all of it.

Does that answer that question?

JANIS KARKLINS: Thank you, Chris. I think somewhere lower in the case, there is a mentioning that that specific data will be requested.

Alan Woods, please?

ALAN WOODS: Thank you, Janis. I just want to perhaps support Chris on this one, anyway. I think it's very clear that, in whatever we come up with , and possibly something we should be thinking about in policy recommendations, is that a person who's requesting data should never be requesting the entirety of default by default of the data sets. It will be based on the case that they are specifically requesting. That is going to have to be one of considerations if there is a 61F-type review of it because it should be limited and specific and (to use the word) necessary to the specific case. So I think Chris is building into that, and, if I understand from what he said, it is important that it would be on a case-by-case basis. I wanted to support him on that. Perhaps that is actually [true].

JANIS KARKLINS: Thank you, Alan. I think that, with this understanding, we can move to the next sub-item, and that is Sub-Item D. Sub-Item D

speaks about the lawful basis for disclosing of non-public registration data to the requester.

Any comments on this? Alan? Or that is an old hand?

So we agree that 61F is the lawful basis? 61F of GDPR, which says processing is necessary for the purpose of legitimate interests pursued by the controller or by the third party, except where such interests are overridden by the interests of fundamental rights and freedoms of data subjects which require protection of personal data, in particular where the data subject is a child?

Let us move now to "e": supporting info to determine the lawful basis for the requester. Any comments?

Alan, your hand is up.

ALAN WOODS: Sorry, Janis. My hand went up in relation to "d." Just very quickly, it was more of an illustrative point for everybody on this one, that this is an absolutely important consideration of why you were doing these case studies. In this particular instance, in the way that Chris has put this, [inaudible] specifically because we're talking about LEA access outside of jurisdiction. So we're talking about something along the lines of the FBI asking somebody in Ireland. It is very important that, under this instance, there is a difference between the reason why they are asking for it and the legal basis by which we are going to process that data.

In this specific case – I think this is where then delineations are important for us – this is a 61F, but in other LEA cases, it's much more straightforward, where we could have a legal obligation to do it. So I just wanted to point out that this is a very subtle and very important point in this specific case study. And this is the value of these case studies, not necessarily getting as many as possible at the moment. So I just wanted to point that out when I had the opportunity. Thank you.

JANIS KARKLINS: Thank you. Another Alan: Alan Greenberg.

ALAN GREENBERG: Thank you. I'm confused by that last comment. I thought this use case was E.U. law enforcement in a non-E.U. jurisdiction. It's not clear to me under GDPR. E.U. law enforcement has specific rights. It is only against controllers within the E.U. jurisdiction? I would have that this is a law enforcement one, not a 61F.

JANIS KARKLINS: Alan?

ALAN WOODS: Thank you. Sorry. Very true. If this is E.U. law enforcement – actually, that's a very good point – asking somebody within the E.U., it actually [inaudible]

JANIS KARKLINS: Outside E.U.

ALAN GREENBERG: It's outside the E.U.

ALAN WOODS: Say again? Sorry.

ALAN GREENBERG: The use case is E.U. law enforcement asking for data in it for a controller outside of the E.U., as I read it, but I would have thought the GDPR E.U. rules still apply to the privileges given E.U. law enforcement. Maybe not.

ALAN WOODS: I think Chris is probably best to answer that one, but if you were in E.U. law enforcement, you have no powers to ask a U.S. company. Just because you're law enforcement doesn't mean you have that power, but you can still specifically ask, because of my position, because of my authority, because of that which I am doing, if I am to be believed and trusted as an upstanding member of law enforcement? Well, then you should consider that under 61F if I am requesting European data. I think it works [inaudible] in the situation that I had in my brain, where it was a non-E.U. law enforcement asking of an E.U., or indeed somebody outside the E.U. but it is E.U. data. I see your point, but I think this still applies. This would be a 61F because we would have the ability to consider it under 61F.

ALAN GREENBERG: To be clear, I wasn't making a point. I was just asking a question.

JANIS KARKLINS: Thank you. Maybe Chris can help us to clarify those questions. Chris, if I may ask you another one, shouldn't we, in relation to this discussion also, think what would be the legal purpose/lawful basis in an opposite case, when a non-E.U. is asking an E.U. entity for data? We can think of other combinations.

CHRIS LEWIS-EVANS: Thanks, Janis. The second case goes to flip some of those things just for that exact purpose. Going back to Alan's conversation around legal basis, Alan was absolutely spot-on there. If myself as a U.K. law enforcement was to ask Alan within another E.U. country for this data, I would be acting under my own legal basis, which would be the Crime and Courts Act. But that has no jurisdiction outside of the U.K. So within Ireland for Alan, that would make any difference to him, and that doesn't give me any rights to compel him to do anything. Therefore, his lawful basis would be under 61F. Mine for the processing would be my own [inaudible] Crime and Courts Act. Then maybe Section 7 to actually ask for the data, and then process it, it would be under the Crime and Courts Act. But Alan's lawful basis would be 61F. That would work across the E.U.

Realistically, that will also work for non-E.U. into E.U. As I think Marc pointed out earlier, we just then get into the field that we've not touched on yet, which is the whole transfer of data across

jurisdictions as well. The legal process I think is quite clear on that. I hope that answers any questions people had on that.

JANIS KARKLINS: Thank you, Christopher, for clarifying. I see Hadia is asking for the floor. Hadia?

Hadia, please go ahead.

HADIA ELMINIAWI: Hello?

JANIS KARKLINS: Yes. Please go ahead.

HADIA ELMINIAWI: What about an investigation of a criminal activity against a victim not in the jurisdiction of the investigating E.U. law enforcement agency? Because we have covered the criminal against the victim in the jurisdiction of investigating E.U. law enforcement agency requesting data from a non-local data controller and from a local data controller. But what about victims not in the jurisdiction of the investigating E.U. law enforcement agency?

JANIS KARKLINS: Chris, could you elaborate on this issue?

CHRIS LEWIS-EVANS: Yeah, I could try to. That would become very difficult – why a law enforcement person is investigating on behalf of the victim outside of their won jurisdiction. That would probably down to your local law: if you can investigate on behalf of a victim not under E.U. jurisdiction. There are cases where we investigate certain types of malware where you might not yet have identified a victim within your own country but you know of victims elsewhere. Realistically, you'd have to ensure that you have your own legal basis in your country.

I think, with the way that this is described, it would be under the same thing. As long as us as a law enforcement agency has a lawful purpose to cover that investigation, we would be covered by that. Then any requests for any data would fall under 61F if that data controller was outside our jurisdiction. If they were inside, obviously we may rely on one of the other lawful bases. [inaudible]

JANIS KARKLINS: Thank you. Not simple. Thank you, Chris. Let us move to Sub-Item E. Any comments?

I see none. Then Sub-Item F.

I see Alan Greenberg. Please go ahead.

ALAN GREENBERG: Thank you. I guess I'd like to understand why the first bullet is there. If we were talking about E.U. law enforcement within the E.U., clearly they could subpoena or request any data held by the controller. So I'm just curious why this one specifically says not

any past data. They have no control over whether the controller has past data or not, but if there is, I'd like to understand why it is excluded here.

JANIS KARKLINS: Thank you, Alan, for your question. I will see if there are any other questions or comments on the topic.

I see Greg Aaron.

GREG AARON: I was going to respond to Alan. I think there may be an assumption here, which is we're using a protocol to make a request and then a response. So this is excluding the idea of who was. You're just making a query for what is currently in the registry, for example.

JANIS KARKLINS: Alan Greenberg, are you satisfied with his answer?

ALAN GREENBERG: Thank you. That's certainly true assuming we're talking about automated RDAP requests. Does that imply there might be another use case looking for past data which clearly could not be automated?

JANIS KARKLINS: Chris?

CHRIS LEWIS-EVANS: Thanks. This is relying on the 61F, where there's now compulsion and it goes under a balancing test. Realistically, when we talked about this within the GAC, what we're looking for is what is akin to the WHOIS data as was. What we're not asking for is all the information that the registry or registrar may hold on the data subject. If we wanted historic and any other information they had, then we would be going down a court order. So that would be under a separate process – so outside of this user case.

I think, when we start getting into historic information and extra information, that is when we're into the court orders of territories – so outside of this sort of process. And definitely outside of automated [inaudible]

JANIS KARKLINS: Thank you. Very clear. Any other questions on F?

If not, then we can move to G: safeguard requirements applicable to the entity disclosing the data. Any questions or comments on G?

I see Brian. Brian King?

BRIAN KING: Thanks, Janis. I'm curious about the penultimate bullet there, that the entity disclosing the data has to perform a balancing test with the right to object and to erase. Maybe we need to flesh out how that should work. If we're looking for automation here [or]

standardization, I'm not sure that that bullet works for that. I'd love to hear what Georgios and others think there. Thanks.

JANIS KARKLINS: Thank you, Brian, for your question. Let me take questions or comments from interested parties and then ask Chris and Georgios to respond.

Alan Woods, please?

ALAN WOODS: Thank you very much. I had a point myself, but I'll just go straight into what Brian is saying there. Absolutely, you're 100% right. The balancing test and 61F is the largest issue that we have. We've been saying this for many a month, that it's impossible or very unlikely and very hard to automate the balancing test because that needs to be done. That's what's written in 61F, into its very basis. So yes.

My own point there was in relation to the last bullet point. I have misgivings about the "must disclose," especially when it comes to a law enforcement one. I think there are instances where we should definitely disclose to the data subject, but I think, when it comes to law enforcement, we need to mindful of the fact that there might be instances where might be also prevented from disclosing. So the concept of a "must" in this one we just need to soften, possibly as "where possible" or something like that. But generally speaking, I agree with that.

JANIS KARKLINS: Thank you, Alan. Milton – oh, sorry. Marc Anderson first, then Milton.

MARC ANDERSON: Thanks, Janis. My point was actually going to similar to Alan's. The last two bullet points talk about "must disclose," and then the sub-bullet point also talks about how there must be a mechanism for implementing the need for confidentiality for the ongoing investigations, which I think was the point Alan was getting to there. This is a topic I don't think we really have delved into a lot: when the data subject can, should, and has a right to know who's been requesting their data and when the requests for the data subject's personal data need to be held as confidential.

I agree with the points Alan made. I think this is an important topic that we need to maybe flesh out a little bit more and one we really haven't gotten into in detail yet. I think I'd be curious as to what Chris's take is on this, maybe what he envisions as scenarios where it would/wouldn't be necessarily to treat as confidential, and how we can incorporate that into our work.

JANIS KARKLINS: Thank you. I think that Chris wrote that is he happy to put "may." Milton and then Georgios. Milton, please?

MILTON MUELLER: I was just noticing that Brian used the word "automated." I wanted to just echo what Alan said. I just don't see how a balancing test can be automated. Let's suppose you're making a request for

10,000 domains for some reason. There could be a balancing test that does the initial gatekeeping which is not automated and then you can automate the process of delivering the data afterwards. But I don't we should be assuming that all of this can be automated. I'm very uncomfortable with that assumption.

JANIS KARKLINS: Thank you, Milton. Let me maybe give a chance to Georgios and Chris to speak. Georgios?

GEORGIOS TSELENTIS: Can you hear me?

JANIS KARKLINS: Yes, very loud and clear.

GEORGIOS TSELENTIS: Okay. Just about the additions under all this bullet point on safeguards regarding the balancing test, I think it was mentioned from Alan Woods that this particular use case has the [inaudible] to deal with 61F as a legal basis. We all agree that this is maybe the most interesting one. It is natural to have under the safeguards a section which is dealing with safeguards regarding the balancing test that they're going to perform.

Now, having said all that, this is the first iteration of what we could come up with. I can understand some of the concerns mentioned about the automation of the balancing test, whereas I'll let Chris talk to this because I think this is in case we have a recurring

similar request for disclosure. I can see the practical problem of running a balancing test which is practically the same. It will be very helpful to have something in place, but I think this is something that can be debated. It can be discussed.

As I said, the important issue is that we need to have safeguards regarding the process of the balancing between the rights of the registrant and the rights of the ones who want to disclose the data. It may need to be a little bit more fleshed out. In this sense, we need some more input if people have concerns on those. I'll let Chris talk about the automated because this is not my cup of tea.

JANIS KARKLINS: Thank you, Georgios. Chris?

CHRIS LEWIS-EVANS: Thanks, Janis, and thanks, Georgios. I think, as we've seen from some of the models that we had presented to us in Marrakech, everything has to have a balancing test in the 61F. Can we do that balancing test ahead of time? It's a very difficult question. I don't think we've got there yet, and I think that's certainly going to be one of the policy considerations going forward about how we can do that. But realistically, without being able to do that balancing test ahead of time or repeat it for 100 domains that you've asked for the same user case for the same reason, then that's realistically the step we need to overcome to get to some form of automatic system.

Just to go to the "must disclose/may disclose/should disclose," I'm quite happy with either "may" or "should." It doesn't really make

too much difference to that. What I'd like to see is some form of communication between the contracted party and the law enforcement agency. Certainly within the U.K. we have a point where we had to disclose everything that we've done when it comes to court. That's something that we have to do. Once we get to that stage of investigation, then we could maybe go back to [inaudible] and say, "We are at this stage. You may now disclose this." So that's pretty much into the implementation phase, but that's something that definitely needs to be done around that disclosure and confidentiality side.

JANIS KARKLINS: Thank you, Chris. We have about five minutes to go on this call. Again, we have not exhausted our agenda. Let me see if we can quickly listen to three interventions. Three hands are up now – Hadia, Alan Greenberg, and Margie. And then we will draw the line on this discussion today and we'll resume it during the next meeting.

Hadia, please go ahead.

Hadia?

While Hadia is trying to mute, Alan Greenberg, please go ahead.

ALAN GREENBERG: Thank you. I think one of the questions we're going to have to tackle at some point and probably need legal advice on is to what extent a balancing test can consider the credibility and trustworthiness of the requester because the issue that you can't

automate things presumes that you cannot trust the requester. That's a question that I think we need legal opinion on because the whole concept of automating any of these processes presumes that, through authentication and accreditation, the requester has some credentials that we believe we want to honor. Thank you.

JANIS KARKLINS: Thank you, Alan. If you could then write the question and pass it to Leon for putting it on the agenda of the Legal Committee.

ALAN GREENBERG: I'll do that.

JANIS KARKLINS: Thank you. Hadia, you can speak now?

Hadia, please go ahead.

We don't hear you, Hadia. At least I do not hear.

Okay, thank you. Margie, please go ahead.

MARGIE MILAM: Hi. I was going to say something along the lines of what Alan Greenberg said. I think we cannot assume that you have to have a manual review of every request under 61F. That's the reason we have [questions] from the Legal Committee to outside counsel. Once we have those answers, then I think that'll help shape the

answer to this section. This is something that we will need to address in any use case: the question of whether you can have a potentially automated system and a pre-authorization, assuming that you have appropriate safeguards and contracts and identification of the notifiers of the people asking for it. So this is going to be an ongoing discussion. I just wanted to flag that we don't agree with the approach that Alan Woods suggested and that we'll have to have a pretty long conversation, I think, about this. Thank you.

JANIS KARKLINS: Thank you, Margie. I think we need now to leave the conversation here because we have one minute left for the meeting. If I may ask team members to look again to this case, starting from G down, and provide any concerns or questions you may have in writing by Tuesday that Chris can incorporate maybe in the next, if they will be need to incorporate them, edited version of the case. We will start examination of this case with the Sub-Point G during the next call.

I don't think I have time to ask Caitlin to restate all the action points. I will ask Caitlin to send those action points to the mailing list. With these words, I would like to thank everyone for active participation. We'll talk about in one week's time. Thank you very much. This meeting is adjourned.

[END OF TRANSCRIPTION]