ICANN Transcription
GNSO Temp Spec gTLD RD EPDP – Phase 2 LA F2F Day 2-PM
Tuesday, 10 September 2019 at 15:30 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.
Attendance and recordings of the call are posted on agenda wiki page:
https://community.icann.org/x/6oECBw
The recordings and transcriptions are posted on the GNSO Master Calendar Page: http://gnso.icann.org/en/group-activities/calendar

JANIS KARKLINS: Good afternoon. We are starting our conversation about legal memos of Bird & Bird. We got very quick turnaround from lawyers and we have now about 40 pages to read since last night, and then [last one fell in] just a few hours ago. One hour ago, actually. But all of them are relevant to our conversation and therefore I, not being a lawyer, would love somebody from legal team would take over the responsibility and kind of handle that conversation. But if not, then at least to launch it.

And in that respect, León kindly agreed to introduce the memos and launch the conversation. I think the aim of this conversation would simply be exchange views how the information provided or legal advice provided by Bird & Bird will or can influence our conversation about the SSAD and different aspects of functionality of the standards we're trying to develop.

So with this, I turn to León for introductory remarks.

LEÓN SANCHEZ: Thank you very much, Janis. You know it's always the lawyers' fault, so don't shoot the messenger.

JANIS KARKLINS: You're both.

LEÓN SANCHEZ: Exactly, I'm both. I think we've received feedback from Bird & Bird on the first batch of questions that we submitted for their consideration. There are some aspects that I think is useful to highlight. Of course, the aim of these highlights is not to focus the discussion on these supercyclic highlights but rather to, as Janis rightly said, set the scene for a more robust discussion on the legal memos. I don't know if everyone has had the opportunity to go through them, certainly not in detail but at least browse through them and get the chips of knowledge that they offer.

For example, in terms of the discussion on controllers, I find useful that it states that entities cannot assign or disclaim controller status unless the status assigned by law, the status flaws from actual controller over key data processing decisions. I think this is a useful bit. There are a couple of other more like for example in their summary in one of the memos, they state that CPs are controllers, and given ICANN's role in determining purposes and means of processing, that they will be joint controllers with ICANN Org in respect of their disclosure of registration data for requestors via SSAD.

So I think this is a useful piece of information again. I don't want to take more time highlighting what I believe is useful, but rather would like to open the floor for a broader discussion and exchange of thoughts in regard to these legal memos that we got. So I'm now going back to you, Janis.

JANIS KARKLINS: Yeah. Thank you, León. And of course, for me, not being a lawyer, I would love to hear opinion of different groups how that statement that ICANN and contracted parties act as joint controllers impacts our sort of discussion on the standard itself. So that would be useful to link those two issues together, and certain extent, that will determine the final shape of the model whenever we will get there.

So I have Volker, Brian, and Hadia in that order.

VOLKER GREIMANN: Thank you, Janis. And I must admit I didn't have the time to read the entire memos in depth yet because I was dead tired yesterday when I got home, and I just had a little time to fly over them, have a general overview. But I was impressed by the fact that nothing in these memos that we received was entirely new to us. Basically, everything they said was use more words to express the facts that been expressed by the registrant lawyers, European lawyers and others on the EPDP team which they had been expressing all along. So we could have saved a lot of money by just believing us. Maybe we'll try that for the future.

We are experts on the GDPR in our companies for a reason, and when we say something, it might be good for the entire group here to not just see that through the lens of a contracted party or the other party's thing, what is convenient for them, but rather, trying to reflect what we believe actually to be the law.

JANIS KARKLINS: Thank you, Volker. Brian?

BRIAN KING: Thanks, Janis. There's a couple things at a high level that I'd like to point to and then some other conversation I think we can have from that. The first really interesting thing for me in the first legal memo is that Bird & Bird pointed out – as I think we suspected, but this is the first time we got this in writing – is that a contracted party's liability under GDPR is significantly affected by whether it's a controller or a processor. And as you can imagine, the liability is significantly higher if the contracted party is a controller as opposed to a mere processor.

I would maybe request that we take back to the legal committee and run by the plenary a couple of follow-up questions on the analysis in the Bird & Bird memo, particularly about the analysis that yields the result that the contracted party is currently a joint controller with the way that the fats are today. I don't entirely disagree with the facts that they looked at to come to that conclusion, but I think it's important for this group to consider that we're creating a policy for tomorrow and how these relationships work and how the contracts between contracted parties and ICANN Org will work, and that the status quo today need

not necessarily be the status quo tomorrow. And in fact, it could be better for the contracted parties tomorrow than it is today if contracted parties wanted to be processors as opposed to controllers.

One thing in particular I would press on with Bird & Bird is that of all the factors that they looked at to evaluate whether contracted parties are controllers or processors today, most in my mind seemed to indicate the contracted parties are merely processors. The one that Bird & Bird seemed to hang their hat on was that the expectations of the registrant are such that the registrant would think that the contracted party is a controller and would make the disclosure decisions.

I think that's a particularly weak point to really focus on, and Bird & Bird says traditionally contracted parties have been seen as the controller. And traditionally is an odd word choice considering this has been happening for about a year. So I think I would really press on that a bit and then we could take conversation from there. Thank you.

JANIS KARKLINS: Thank you. Hadia, please.

HADIA ELMINIAWI: So if we look at the memo and take it as it is, it says that joint controllers – page 7, 3.2, does not necessarily mean that the parties each have to [undertake] all elements of compliance. So being joint controllers does not mean that both parties will undertake elements of compliance, and they go on saying that joint controllers must determine their respective responsibilities for compliance in particular as regards

to the rights of the data subjects and their respective duties to provide information by means of an arrangement between them.

So my question to the group, could we take it from here and start working on that part if the group agree that you are joint controllers, then according to the memo, you should be starting to talk with ICANN about the respective responsibilities of compliance and who's responsible for what. And I think that could be the starting point.

JANIS KARKLINS: Okay. Thank you. Next is Matthew.

MATTHEW CROSSMAN: Thank you. Just a couple points to respond to some of the things that Brian raised. I don't think it's a question of whether we want to be controllers or want to be processors. It says in the memo this is a factual determination. It doesn't have anything to do with what we want. It has to be based on the facts.

The second thing is when we talk about – if we do want to dive into this question of contollership or whether contracted parties might be a processor, I think it's really important to pull out from this memo that the presumption is of controllership. That's the place where you start, and you have to overcome that presumption to show that you're a processor.

So I tend to agree with the analysis that contracted parties are controllers, but if we want to have that discussion, we need to start from that presumption of controllership.

And the third thing I want to say, I disagree that data subject expectations are a weak basis to find controllership. The whole point of GDPR is that we should start from the perspective of the data subject expectations. In my mind, that is fundamental to the purpose of GDPR, and so I think in a lot of what we do – and actually, I really like this about the memo – it talks a lot from the perspective of the data subject, and I think it would be useful for us to remember that as we're having the discussion that we really should be thinking about what the data subject expects and thinking about it from their perspective when we're making decisions.

One last thing. To Hadia's point that if we are joint controllers we should be having these discussions with ICANN, we are. There's a group of contracted parties – and I think [Allan] updated on this yesterday – that is working through the roles and responsibilities of the parties in this arrangement.

We sent a draft over to ICANN with the way we thought the roles would be allocated. There's been some back and forth there. So that process is happening. Thanks.

JANIS KARKLINS: Thank you, Matthew. Stephanie followed by Thomas.

STEPHANIE PERRIN: I just wanted to point out that the roll of processor versus controller's been around since 1991 when the original directive was tabled, and not much has changed in the new regulation except for the specificity of

how you must arrange your liabilities. So really, we should have figured this out a while ago. Thanks.

JANIS KARKLINS: Thank you. Thomas, then Chris, and Dan.

THOMAS RICKERT: Thanks very much, Janis. A quick follow up on what Hadia said. I guess this is pretty much what we've been trying to achieve in the discussions that we had. You might remember when I stepped to the drawing board yesterday, I said we can have joint controllers and then allocate functional responsibilities. That's exactly what's being discussed here.

So the registrar who collects the data shall have the responsibility of informing the data subjects about the processing. That's something that a registry can hardly do because they don't have the direct window to the registrant. So you go through this processing, and this is why it's so interlinked, what we have worked on in phase one, that we actually go through the various responsibilities and say, "Okay, data [rectification] requests are being dealt with by joint controller A, B, C" or whatever might be the case.

So I think this is a confirmation of the analysis that we've been discussing from the get go. My question to this group is, and I mean this very generally, are we now having this memo in front of us in a position to say, "Okay, we're going to follow the advice that we've been paying for?" Because I think what we want to see the least is now we're trying

to tear this apart and have competing legal opinions in order not to trust what's in here.

I think we spent a lot of money now – luckily not our personal money but we spent a lot of the community's money to get independent legal advice. There we have it. And I'd really like – maybe Janis can conduct this at the end of the meeting after everybody had a chance to consult with their respective groups, are we now committing to following the independent legal advice and just operationalizing it? Because I think if we don't do that, we're going to get nowhere. That was at least the idea at the very beginning.

JANIS KARKLINS: What was the question?

THOMAS RICKERT: Brian asked whether I consider this independent legal advice. And I think we should maybe take it for that. But discussing questions such as this shows that probably we're not in a position to even settle on that. So that's money wasted. If we find out that nobody's going to trust what we have in front of us, then it's a futile exercise. Then we should stop bringing in external legal advice and have the courts decide. That's what we heard from the CEO yesterday, that's what we've heard from others.

I thought that we would be asking for external legal advice – in order not to call it independent legal advice to get some third-party arbitrator, let' say, to help us overcome the discussions about some

which I think GDPR related questions. There we have it. What are we going to make of it?

And I don't mean to be difficult and I hope that you don't see it as that. I'm trying to be as constructive as I can, but I think we would all benefit form agreeing on having one source of wisdom, let's say – and it can be Ruth and her team to lean on and work on the basis of that.

JANIS KARKLINS: Thank you, Thomas. Chris D.

CHRIS DISSPAIN: Thank you. Does anyone object if I make a comment based entirely on my experience as a lawyer and nothing whatsoever to do with being a board member? And clearly someone in this room that has no skin in this game other than simply being here. Anyone have a problem if I do that?

UNIDENTIFIED MALE:

CHRIS DISSPAIN: Actually, no, if someone objected, I would take them outside and discuss it with them quietly. Exactly. No, there's no going back from the edge. So my take on this is that it is about determination. You clearly can't choose, it will be determined.

I think that what Bird & Bird are saying that you could argue – there are arguments that you could put that in certain circumstances, the contracted party would be a processor, but that the weight of legal discussion and argument is that actually they would not be, they would be a controller and therefore in these circumstances, joint controller with ICANN.

They do say that there is a directive coming in possibly six months, which [inaudible] guidance of some description which may have a distinct effect and may actually change that, but they are saying "If you ask us to tell you now what we think, generally speaking what we think is that it will lean towards joint controllership."

Now, what you guys choose to do with that advice, I think I'm going to put my ICANN hat back on for a second. Volker, you said we spent a lot of money and it would be nice if everybody just believed what we said in the first place because we're experts. And I kind of expect that you're experts, but I do think we need to understand it's actually very important for all of you as well as for us that there is independent – in the sense of not us – advice rathe than simply accepting that one person in this room or two people in this room have legal experience in the field and can say something. I just wanted to address that point, it's not meant to be in any way critical.

As for how we move forward, it's a hard one because you could argue that – I think it's important to treat the advice as being effectively there and not tied to anybody. Yeah, okay, we're the client, ICANN's the client, but really, you ask the questions and Bird & Bird have replied. So

I suggest it's worth remembering it that way. Where you go from here, I'm not commenting on. Thanks.

JANIS KARKLINS: So we're going home probably tomorrow. Dan, please.

DAN HALLORAN: Thank you. Just two notes of caution. One, not everyone's had time to digest these. [inaudible] there was a lot of late night reading, and kudos to the people that have been able to parse through quickly and pull out these useful tidbits. That's great, but I think it'll take all of us time to read through it a couple times more carefully and outline it, analyze it and understand it.

Another note of caution is that I understand this to be advice Bird & Bird's opinions, which I have utmost respect for Ruth Boardman. I think we're all really lucky that she's looking into this for us. But these are hypothetical questions about if we build this hamburger, how would it work. And assuming we build in certain stuff, this isn't analysis about the current situation or the phase one recommendations or how the relationships between the parties work in the pre-hamburger phase that we have today. So I don't know that we can take what she's saying here and apply it to the phase one stuff. And thanks, [Allan] and Matthew for going into what's going on about implementation of phase one, but these memos are about phase two and about the hamburger which is still hypothetical, and I think until we really know how the hamburger's going to work and what is ICANN Org going to do, what are the condiments, if we're going to have condiments, what are they going

to do, you can't analyze who's going to be a controller or a processor, if this is going to be independent joint controllership, until you know the facts of how the process is going to be handled and who's going to be responsible for what. Then you can determine who's a controller and who's a processor if there's joint controllership. Thank you.

JANIS KARKLINS: Thank you. James.

JAMES BLADEL: Thanks. I'll just be brief and just to kind agree with Thomas for the most part. I do agree, Dan, it's early and we have less than 12 hours on these, so let's take a look at them. But I also want to just kind of emphasize that we went out of our way to find what we all I think agreed was a very competent firm that had a lot of expertise in this area and we all agreed on the questions that would be sent to them, so let's not presuppose that here's something wrong with the advice, that it's not independent or that we need to get clarification on the answers because we asked the question incorrectly. Let's take it at face value. We went through a lot of trouble to get this, and the idea was this was supposed to break through a number of impasses that we'd reached as a community. And I think that we need to take it onboard and treat it with the weight that it deserves, and in proportion to the care and effort that went into selecting them and getting this advice.

So I'm just concerned that I feel like we're questioning the validity and independence now of the advisors when I don't think that's appropriate at this stage.

JANIS KARKLINS: Thank you, James. Margie?

MARGIE MILAM: Same thing, I haven't had the chance to really absorb it, so I don't know yet how I feel about what's said here, but it strikes me that having been at a law firm before, in something as new as GDPR, there's basically reading the tea leaves based upon what we know now, what cases there are now.

So I think what would be most instructive is what comes out of the communications from the data protection board, because they're the ones – and then what if they come out with a different answer? I don't know. Maybe it'll be the same, but it's clear that the Strawberry model and the communications with the data protection board are posing a system where it looks to me – and I don't know, Dan, maybe you can confirm this – that they're trying to change the roles and responsibilities so that it's more likely that the contracted parties would be processors rather than contractors.

I think what Bird & Bird is talking about here is the current situation, but as Brian mentioned, we're in the unique opportunity of being able to redefine roles and responsibilities. And if that passes muster with the data protection board, then we might end up with a completely different response and results than what comes out of the Bird & Bird memo.

So I'm just floating ideas. I don't know whether that makes any sense, but I do feel like whatever we get from them would be far more instructive than what came from the memo.

JANIS KARKLINS: Thank you. León?

LEÓN SANCHEZ: Thanks, Janis. Just to reinforce what James was saying, we got our feedback from our independent advisors. Trying to question independence and rehash questions until we get the answers that we expect to get is not good for anyone, so let's take the advice at face value as James suggested, and focusing in trying to use it as a useful input for our deliberations.

JANIS KARKLINS: Thank you, León. Allan?

ALLAN WOODS: Thank you. Two points. First, to Dan, obviously I agree we need time to digest this memo, but from the reading of it, I would just say to you that they didn't go in on an assumption, they started with the case law and how [inaudible] as seen at the moment as to controllers and processors. So I wouldn't dismiss it just yet on that. I think we should definitely discuss this in our group. [Sorry, I was taking the other side] on that one.

Now, to go to Margie's point, I understand that what's in this memo might not necessarily be what was hoped, in fairness, from your point of view. I do think that – I'd like to draw, I suppose, an analogy, a statement that was made by Helen Dixon at an IAPP conference where she said that the – and I'm paraphrasing big time here, obviously – DPA is the data protection authority, not the data protection advisor.

She said if you want to get a knowledge as to whether or not you're in line with the law or not, you get legal opinions. You ask your lawyers. You don't ask the DPAs. And I know we're in consultation with the DPAs, but we cannot wait for them to tell us what to do here. We're here to make that decision and this is the legal advice that we have been given.

So I think that we need to not hedge our bets anymore. We have a very small timeline here. I think we need to just take what we have and work with it in the best possible way so that we can make this process a lot easier for you.

We're all sitting at the table so that we can make it more predictable, a better way of getting disclosure of this data to achieve purposes that we all believe to be valid, we just need to figure out a legal way of doing it. This is the playing field that we are now on, and I think we need to embrace that and move forward, and let's not put up any more roadblocks of "Maybe we'll get different advice in future." Unfortunately, it's not something that we can rely upon.

I just caution- I know you have to read it properly. So thank you for that.

JANIS KARKLINS: Thank you, Allan. Chris?

CHRIS DISSPAIN: Thank you. I suggest that [we're about to] ask DPAs questions. We had a whole thing about that yesterday. I'm game to accept that the Bird & Bird advice is 100% correct. Let's just assume that for a second. But if you look at the Bird & Bird legal advice, there are a couple of escape clauses in there, if you will. Not about their advice but simply there are circumstances in which it might be possible that a contracted party could be deemed to be a processor even though it's leaning towards them being a contracted party.

So it's not impossible that the DPA guys come back and say in general terms normally in these circumstances, they would be a whatever they are, joint controllers, etc., but the way that this has been put to us and the way that this model is working, we'll be prepared to accept that they are processors.

You might say they'll never say that, you might say it's not the sort of thing you're going to get out of them. I have no idea. But the point I would make is we are asking them, and I just wanted to slightly push back on "We don't have time to wait." I think there is a lot of stuff for this working group PDP to do on the policy and what the requirements are and what depth of data would an intellectual property person be entitled to and what depth of data would a law enforcement person be entitled to, and all of that stuff. And we could quite simply wait a little bit and see what the DPAs say. That's my two cents' worth and I shall not say another word to day. Thank you.

JANIS KARKLINS: Thank you. Thomas?

THOMAS RICKERT: Yeah. My jet lag is kicking in quite conveniently, but this discussion really makes my blood boil. I think when we started working on this, and even before the EPDP days, [we were] all about let's try to find a defendable solution.

Dealing with legal stuff, you know that probably you're not going to have a perfect solution or a solution that might need to be adjusted as time goes by. But to say "Let's wait for another six months until we get this opinion from the European data protection board," who's going to – nobody's going to benefit from that. The European data protection board will not issue a paper saying "For ICANN, this is going to meet this and that." It is going to be yet another paper, ink on white trees, that gives enough room to speculation. And everybody will cherry pick what they like best and what they don't like.

So let's stop this, or let's end this meeting now and all go to the beach and wait for this paper to see whether it's going to miraculously answer the questions for us. How much more evidence do you need? The European data protection board in its letter to ICANN has said "You are likely joint controllers." Then they've put it in writing recently again. Bird & Bird said it's the likely scenario. What more do you need to be convinced that this is a defendable solution the least?

Let's start operationalizing that and adjust as needed, but let's not wait for some moment where everybody has a different idea of what that moment or event might be to come up with a perfect solution. You're not going to get that. It's legal stuff, you need to make one solution work.

And back to Brian's point, starting from the users' perspective. As I mentioned, when I was at the whiteboard, Article 27 was done exactly for the purpose of saving the data subjects the trouble of trying to identify who has what role in a very complex online game. That's what we have.

So I urge you, let's stop this game of pointing elsewhere and waiting for stuff. Let's get this written up and then you have something that you can start a good discussion with the data protection board with. And when we hear the European data protection board, they're giving us advice and we're the only ones who are privileged enough to get advice.

If you read between the lines, they are fed up with ICANN. They said "Do your homework, and then we have something to talk about." And we have not done our homework. We have not put anything substantial in writing. So let's get over this, let's write something up, and let's discuss a work product rather than speculation.

JANIS KARKLINS: So I think that we're trying to put something in writing and zero draft is something that we are starting to write up. So I have Dan, then Milton, then Alan, and then Stephanie and then Margie.

DAN HALLORAN: Thank you. Just quickly to go back to Allan – and sorry to have these back and forths – I want to correct any misimpression that I wanted to dismiss anything. On the contrary, my first read was they're excellent memos, good analysis. I was just saying we're going to need time, I think, as a team to let it digest.

And then also, my second point was that these memos are about hypothetical hamburger, they're not looking back at the phase one status. This is a complicated – like Thomas is saying – joint platform with hamburgers and condiments and patties and buns, and it'd be difficult to untangle it. So it's analyzing that hypothetical hamburger, not looking back at our phase one in the current situation, at least this memo.

JANIS KARKLINS: Milton, please.

MILTON MUELLER: Yes. Very briefly, I agree with Thomas. My blood is not boiling, I'm just baffled by what the actual rationale is for relying on the DPAs in the way that ICANN Org seems to want to do. It's very clear that DPAs do not act as your lawyer and will not. It's very clear that there are a number of contingencies that would, as Dan was just pointing out, affect the application of the law. And we just have to make the decision. We have a legal opinion now and we've got all kinds of intimations, so we just have to go forward and make the policy in a way that is safely within the parameters of what we consider to be legal. And if we discover later

that we're not right, the problem is not going to be solved by waiting around for the DPAs. It just isn't.

JANIS KARKLINS: Thank you. Stephanie, you want to [inaudible]?

STEPHANIE PERRIN: Just following up on Dan's remark, compared to some of the other data mining systems that the European Data Protection Board and the Article 29 group before them have looked at and analyzed, this is not a complicated system. It's possibly not as transparent as one might want, but that can be fixed. It's not complicated. So I reject that argument, although I do agree we need time to digest it.

I just wanted to point out that one of the reasons that the provision in there for civil society to take a case on behalf of registrant arose out of the [inaudible] decisions where basically the data protection commissioners agreed – were more or less forced by political pressure to accept the safe harbor agreement as being adequate when they did not think it was. And if you doubt me, read their earlier opinion on safe harbor. Nothing changed.

And so the longer that ICANN stacks up the data, the legal opinions – don't forget all the work that we had Chris [Coner] do that we threw out as well, we're just building a case for civil society. If the data protection commissioners come in and come with a different opinion, that's a lawsuit as far as I can see for civil society to say, "Okay, great, the

commissioners are not doing the job they're being paid to do, to look after the interest of the registrant."

So once again, those three risks, legal, reputational and financial, of those three, if I was ICANN, reputational would bother me the most. Thanks.

JANIS KARKLINS: Thank you. Margie? So no flags anymore up. I think we can draw a conclusion to the conversation. So what I understood – actually, not much. One thing is I fully agree that we should not question our own questions. That wouldn't be wise. So we agreed as a team to ask those questions to the Bird & Bird, and we got answers. So we may not like answers, we may use them nevertheless as I understand that there is predominant view that we should use it.

So as next steps, I assume that maybe legal committee during the next meeting try to get in depth conversation about the content of replies, and come back with kind of advice how that could influence our discussion, and so then we will take from there. But please, Brian. You want to say something.

BRIAN KING: You wrapped it up nicely, so I don't want to reopen anything. I think I agree with my colleague Matt here that the user perspective is very important, and I think the memo does a nice job with that in addition to many other things.

The point that I was trying to make to maybe double down on it is that the memo does a great job of talking about what's happening today. And I'm sorry if it comes across as not believing the advice or challenging the advice or not taking the advice, but maybe it's an occupational hazard of being an attorney that you kind of critically read everything that you do read. But the point that I would like for us to consider is that the user perspective could differ. We already have plenty in the registrar accreditation agreement that says what registrants must be informed about and reminded about, and that's a perfect opportunity to influence the user perspective on what it is going into disagreement with the registrar.

So there's a lot of good stuff in this memo. I agree we should take time to read it and digest it, but I just don't want us to be wedded to this as it exists today because there's a lot of opportunity in here, I think, to make this a better system going forward. Thank you.

JANIS KARKLINS: Thank you. What shall we do with other two memos?

LEÓN SANCHEZ: Well, I suggest that we provide space and time for the group to actually go through them, digest them and then have a better informed discussion, Janis. And I thought I heard you say that you would be expecting comments from the legal committee on the memos. I'm not sure that's the task that we were assigned, but if the larger group agrees that the legal committee should go through the memos, analyze them and provide their views, of course, we will be happy to do so, but I

just want to confirm that we're not deviating the original intent of the legal committee.

JANIS KARKLINS: Okay. I take that comment. I withdraw my suggestion that legal committee will do, but certainly then we will revisit all three legal memos at one point during our online conversations as we usually do on Thursday.

So with that in mind, is there any appetite to talk, brainstorm a little bit about the big elephant in the room where the decision of disclosure should be made in the model that we're talking about? Is there appetite for that conversation? Thomas and Allan.

THOMAS RICKERT: I think it's a great and important conversation to have, and it also fits nicely with the discussion that we just had. The balancing needs to be done by the controller, and you need to balance the rights of the individual against the rights of the party that's asserting to have an interest in the data when it comes to 6.12(f), and Allan has kindly put together a paper a couple of weeks back that he shared on the list that I think can serve as a great basis for discussion. But again, if you had a single controller, it would be the controller who had to do that and in a joint controller scenario, you could allocate the functional responsibility of conducting exactly those tasks to one of the joint controllers.

So if we're thinking about contracted parties plus ICANN, and if we wanted to, we could in an agreement designate ICANN or its designees

for that matter to do exactly that exercise. And then once you've done that exercise, and once you've convinced that you've done it properly, then you need to inform the data subjects about this type of disclosure and the rationale for why the balancing test was in favor of the interested party and why disclosure is taking place, and that would need to be transparent to the data subject at the time of collection.

So I think we need to build that into the process. I think in order to provide for a consistent decision making when it comes to balancing tests, it would be advisable to have one entity take care of that. Maybe for our group to come up with parameters and methodology to conduct the balancing test so that you have a consistent decision making whether – it would probably semi automated across the entire industry.

JANIS KARKLINS: So thank you. Allan, your flag was up.

ALLAN WOODS: It was, but to be perfectly honest, I think Thomas has said most of it. All I would say in reiteration is that when we are having this conversation, we must start from the point of view that whomever makes the decisions is the controller or is a controller, and that is kind of the fundamental starting point. So Thomas said the rest.

JANIS KARKLINS: So I understand that the option is that there's a joint controllership as suggested. So as a result, joint, the contracted parties and ICANN needs to decide what would be role of each. And it would be, in my view, a

good opportunity now when we can look each other in eyes to have this conversation. Maybe not conclusive conversation, but at least to thrash out what's the prevailing sentiment in the room, how that could be organized, because that also will have determining impact on how the system would function.

MARIKA KONINGS: Sorry for interrupting, I'm just wondering if it's worth for Allan to kind of walk through what it would entail, because that may help inform the discussion on who would do what if everyone is clear on what the balancing test actually – what is expected. And what is up on the screen is a diagram that was also in the zero draft that was based on what Allan shared at some point to the list, just as a suggestion.

JANIS KARKLINS: Yeah, but let me maybe go back to first impressions. There are a number of flags up, and then Allan, we'll come to you and asks you to walk us through. Honestly, I didn't see whose flags were up first, but let me say James, and then Volker and then Milton, and then Georgios.

JAMES BLADEL: Full disclosure, I don't think I was first, but I do have a question and it's an honest hone. I may be aiming it in Allan's direction if he could touch on this when he walks through, is if we have joint controllers – and forgive me, not a European, not a lawyer, so not a European lawyer – and a controller can make a decision on a balancing test, is the expectation that ICANN, the registry and registrar are going to huddle

and vote 2 to 1 or 3 to 0 on a disclosure? Or "I asked the registrar, they said no, ask the registry, they said no, I ask ICANN, they said yes, jackpot?" Or do I just keep asking until I get the right answer or run out of people to ask? What's the interplay with the different – when you have joint controllers, how do they coordinate those balancing tests? Do they all do their own, or do they work on the same one? I really don't know how that all works, and I'm trying to be sincere without unnecessarily complicating it.

JANIS KARKLINS: So thank you. Volker, please.

VOLKER GREIMANN: Yes. My gut feeling as a lawyer is that not only should it be the controller, but also the controller that has physical access to the data and has probably also the customer relationship with the data subject, which in this case would always be the registrar. And the process of disclosure of the balancing test would always be determined by the legal requirements of that contracted party in this case making the decision of whether to disclose or not.

And I think it may very well be that one registrar develops an automated system or fields for certain types of requests. Automated responses are valid and doable, and [inaudible] types of requests, they are not willing to take that risk and therefore you might have a different response time between contracted parties, but ultimately, the experience should be very similar, maybe the times of handling these might be different because of one registrar might have the resources

available to put a very capable AI on that, the other registrar is a two-man operation that will probably look at this personally. So I think the balancing test, whether it can be automated or not, should be left to the disclosing party, and the disclosing party making that determination is always the one that has the relationship [inaudible].

JANIS KARKLINS: So I hear a little bit divergence of views from the contracted parties. I heard previously that ICANN should be controller and contracted parties processor, and Volker is saying – what I understand opposite – that those who are making determinations are controllers, hence contracted parties should be controllers. Maybe it would make sense to – again, maybe break and then try to have these side conversations among different groups and see whether we can get on the same page. Yes, please.

VOLKER GREIMANN: Maybe just one addition. Ultimately the liability also lies with the person and entity disclosing the data, and that is always the party holding the data, and that's always the contracted party. So between the registration agreement that we have with the customer, the decision making process and the fact that we h old that data, the controllership is highly likely as [inaudible] memos, and I think to change that, we would have to fundamentally change how the registration processes currently work, and I don't think we're set up to do quite that in this EPDP.

JANIS KARKLINS: Thank you. Milton?

MILTON MUELLER: Yeah. I'm glad we're finally discussing this. I have some very basic elements of confusion here. So in terms of my preferences, I kind of agree with what Volker just said, that the registrars should be the point of the decision making for disclosure, but I'm also hearing – just reading the legal decision, there is a phrase in there that says "Under the SSAD, we understand that the contracted party has no means to individually review and then modify, approve or deny SSAD requests. Instead, the system is automated and key parts of the process are entrusted to ICANN Org."

so I think the underlying question behind this is sort of, do we want to build a centralized mechanism for disclosure, or are we talking about setting a set of policies and procedures that registrars would follow? And if we are building this centralized mechanism, does that indeed mean that the registrars have no decision making power? Which strikes me as a bad thing.

So yeah, the reason we would like to see the registrars in the controlling position is because from a consumer standpoint, a registrar's privacy standpoint, we feel like they are most likely to be affected by liability and have the most direct responsibility to the end user, the registrant, whereas the more remote controllers would probably have less of that kind of an obligation. But I'm still confused about this comment within the Bird & Bird legal opinion about automation and what does that mean exactly.

JANIS KARKLINS: So we do not know what kind of system we're building. We're now talking about elements of the system and at one point, we need to determine where that system is. And we can easily say that it may be centralized. It may be decentralized. So we don't know for the moment. The UAM model suggests that in UAM model, that is a centralized system with the automation as a main feature and hopefully everything could be automated. So that was the beginning.

But when we're looking also – and let's assume they were talking about centralized system, the functions that are assigned for the gateway might be very simple just to verify that the request comes in from certified entity or the request comes from uncertified individual. And that's all that this central gateway does, and then it passes information down to the registries or registrars for making determination, and then response comes back through the gateway to the requestor. So that also is one type of centralized model if you wish, but that is not the one that UAM is talking about.

So then we can have compulsory standard where everyone had to sort of join in, or we disagree that that is a compulsory, hence there is no ICANN policy on that. But since the standard and building blocks are developed, then those contracted parties who want to use them may say, "Okay, we will follow them on voluntary basis simply because we think it's workable." So again, these are options that still are ahead of us that we need to determine and discuss in that.

MILTON MUELLER: That does answer my key question, which was, should we be deciding whether this is centralized or not first and then decide who makes the decision, or the other way around. Based on what you say, we should decide who makes the decision first and then decide whether we want a centralized system, right?

JANIS KARKLINS: No, I see it also slightly different. Assuming we're talking about centralized system, and I see here two options here where decision could be made. One option is the decision is made at the gateway level. So the gate determines that the request –

MILTON MUELLER: Janis, why are we assuming that we're talking about a centralized system?

JANIS KARKLINS: Because you're asking me. At least this is how I interpreted your question.

MILTON MUELLER: No. My question is, should we be talking about whether we want a centralized system first, or should we be talking about who makes the decision first? And I was really with you when you were saying things that indicated to me, "Okay, we have to decide who makes the decision first, then we can decide whether it's centralized or not." But ...

JANIS KARKLINS: No, simply I want to explain where I'm coming from and what my thinking on the centralized system – should we agree that that is the case. So I see that in centralized system, one option is that decision is made at the gateway, in other words, at ICANN, and decision is passed on to contracted parties saying "This is determination of controller, please share that information with the requestor."

Another option is at the gateway only ICANN says that the requestor is accredited but please take the request, make determination, decide whether you disclose information or not, and then send it back. So these are two levels where I see determination could be made, should it is a centralized system.

Yesterday we also heard a third option that the determination is made outside ICANN as a theoretical option. Personally, I don't see that this is feasible, but who knows? Maybe it is. So these are my reflections and thoughts on that. I have now three GAC representatives. Georgios is first.

GEORGIOS TSELENTIS: Thank you. I want to make an observation also related to what I've seen in the legal memo, which I think just to summarize our previous talk, I think it's very useful in the analysis. I think everybody agrees to that, that we can use what we have made as an analysis. And if I see there that from the definition of the controller which is the entity that determines the means and the purpose of the processing, if we agree here in this gathering that the processing we are talking about now here

[the] decision, [forget] where the decision is taking place, the processing we're discussing here is the decision, then we have to talk about controllership. And controllership here, in the memo I see a footnote which is also very interesting in page eight, that joint controller must have a legal basis for processing under their joint control. So that's in the footnote.

As I said, as everybody from you, I didn't have time to read the legal memo and go through the analysis, so here we are talking about which entity is now taking the decision, and what is the legal basis under for this decision. And then whether this is happening on the central, noncentral, in parallel. Then we assign the responsibility for this particular processing activity, which is the decision.

And this is a discussion that we have to agree amongst us. We have to say who takes the decision first, and that goes back to what you said, who takes decision for disclosure? So, can we go through this part of thinking?

JANIS KARKLINS: So when we're looking to the hamburger model, question, where the decision is made in reality means who makes the decision, because if we see supply side, that's contracted parties. So when we're taking "where," then it's "who," contracted parties. If we are looking in the interface, so then most likely, that is ICANN. So "where" on the model turns into "who," ICANN.

So this is the question for this session, and again, I hope that we will be able to get a sense of the room how it should be done. So let me go to the next GAC representative, Ashley.

ASHLEY HEINEMAN: It's a total coincidence. Kind of following on this conversation, deciding who and assigning responsibility, I think this ties back to what Thomas was saying, and I think it was quite elegant in that if we find ourselves in a position recognizing a joint controllership situation, we can then assign responsibilities associated with that, including who should be making the decision. And I think if the whole point of this exercise is to introduce efficiencies, which are not in the status quo, quite frankly, why don't we take advantage of that and see how far we can go?

And if that means assigning the decision making role to one entity in this joint controllership arrangement, let's pursue that. Why make it more complicated than it needs to be? If we find out that we can't do that for legal reasons, then we find that out, but I think this is the opportunity to try and make this easy for everyone and as efficient as possible. so I'd like to pursue what Thomas identified here, and with the who's making the decision, a single party, and [inaudible] ICANN as an example, I think.

JANIS KARKLINS: Not sure that I understood. You're suggesting that ICANN should make decision?

ASHLEY HEINEMAN: [Yes.]

JANIS KARKLINS: When we're talking about joint controllership, again, if I understand correctly, so we're talking about a couple. It's either ICANN and contracted parties ...

ASHLEY HEINEMAN: If we have a joint controllership situation – which if I'm understanding it correctly, we can assign the responsibilities in a way that makes sense. What I'm advocating is that we have a single entity in this process make the decision, because I think what's going to be really important is that we do have the predictability in terms of understanding how these decisions are being made. The more parties we introduce into this, it becomes unclear how these decisions are being made, and that I think puts into question the process overall and I think we want to avoid that. That's what I'm trying to advocate, and I apologize if it's not clear.

JANIS KARKLINS: So your preference would be that that is ICANN that makes decision.

ASHLEY HEINEMAN: Yes, sir.

JANIS KARKLINS: Thank you. For once, we had a clear cut answer. So I will take Chris and then I'll take Margie.

CHRIS LEWIS-EVANS: And I agree with Ashley. So what I was going to suggest here is we're obviously looking at how to place this decision to disclose and where it is. I think some of the information we've got about joint controllers is really helpful for that, but what we haven't really discussed is how a centralized system would look. You said there's two types of centralized systems. I don't know whether it would be worth or everyone agrees going through some of the technical models that we've already been presented with and where if we had this sort of system, that would lend itself to a decision being made at this point, do we use the burger as the [inaudible] or do we list the systems that we've seen [technically?] Just a possible way forward.

JANIS KARKLINS: Thank you. Margie?

MARGIE MILAM: Thank you. I agree with what Ashley was saying, and I was going along those lines in my head as well and agreeing with Thomas. Thinking about it from a contracted parties perspective, if it helps with the liability by having someone else taking the decision – in other words, let's just say hypothetically that ICANN was making the decision and that your processing is based on the contractual obligations in the ICANN agreement, I think doing that might actually alleviate one of the concerns that the system, by having ICANN make the decision, is taking away a possible – not completely. No one's going to walk away from this liability-free, but I think actually might reduce the risk associated with

being in the system if you do allow ICANN to make the decision. That's just something to think about, because as I read the memo from Bird & Bird, it seems to say that that's possible.

JANIS KARKLINS: Okay. Thank you. Alan?

ALAN GREENBERG: I've been pretty silent, but I'm trying to listen and understand. And I'm hearing so very different positions on things that we're also told are factual that I'm more than a little confused.

Ashley said if we're joint controllers and we can pick who makes the decision, let's pick ICANN because it's simple. It also has a level of consistency that we're not in a position of registrar shopping to pick the registrar who's not likely to tell anyone anything because the decisions are going to be made consistently.

Someone on that side – I don't remember who it was – said, "Well, the decision has to be made by whoever's closest to the data or closest to the registrant. Volker said we're the ones who hold the data. Yesterday Stephanie said it doesn't matter where the data is, it has more to do with who the controller or who makes the decision.

So we're hearing lots of different things that I thought were factual, and if we can somehow narrow down these options, maybe we can come to closure on something.

Certainly from my perspective, if we can say we're joint controllers and therefore we can assign in contractually or whatever who makes the decision, it makes it very simply, and I believe in terms of liability, whoever makes the decision is liable to pay for it. Maybe that's not the case.

We have too many variables of people stating things as facts that are diametrically opposed. So somehow we've got to get rid of these variations and understand where we are so we can actually makes some decisions. Thank you.

JANIS KARKLINS: This is what we're trying to do. Hadia was next.

HADIA ELMINIAWI: I tend to agree with what Thomas said and Ashley and Alan. Let's look at the ups and downs of each of the scenarios. So we have two options. Either ICANN makes the decision making, or the contracted parties make the decision making.

I've heard Volker say it has to be the contracted parties, but I didn't understand why. I didn't understand the reason behind why it has to be the contracted parties.

And also I've heard Milton saying, "Well, it's a bad thing not to have the contracted parties making the decision making," but again, I did not understand why.

And as I see it, if we have ICANN making the decision making, then there are some benefits on that, like predictability, consistency, ease of use. All those are benefits in my opinion. And let's not talk about liability now, because we're not sure. So we just leave this part aside and focus on the benefits.

So I am with ICANN being the decision maker. Thank you.

JANIS KARKLINS: Thank you. Volker, Brian, and then –

VOLKER GREIMANN: Yeah, I'm glad that you asked that because that's why I put up my sign. I thought it was clear why [inaudible] but I'm happy to say what the basis [of my thinking is.] I fully agree with what Alan G said, that this can be assigned legally, the responsibility for disclosing the data can be assigned to ICANN or any third party, just like any other process can be outsourced.

However, that leaves the liability for that with the party that outsources or contractually assigns it to another party. Since we have the contract with the registrant, registrant will come to us first and ask, "Why did you give my data to ICANN to disclose to a third party? Why did you allow them to do that?" "Oh, we have a contract with ICANN." "Well, that's not interesting for me. I don't have a contract with ICANN so I will complain about you with DPA," and the DPA will make a determination where it should go. And it may go to ICANN, but it will more likely go to us, GoDaddy, whoever. Google maybe.

ICANN has been very clear that they will not take over any liability. They will not indemnify us for any of this. Göran has been making that point for I think a year now. Yesterday again. And from that consequence that we would face that liability, no matter what we agree internally in our contract, and ICANN not being willing to take up the indemnification – and I can't imagine ICANN taking on 4% of the annual turnover of GoDaddy or Google or one of the other larger players that are in this business, from that, logically follows that from a risk assessment position, we cannot afford to assign this to ICANN unless they give us indemnification that they're not willing to give us, and that [inaudible] to give because some of the parties they cannot indemnify because they don't have enough money.

JANIS KARKLINS: Okay. So I think there is already confliction and we need to try to find a way whether this joint controllership may lead to any kind of arrangement that is acceptable to us as a team that we can propose a policy. So I will take Brian, then Stephanie, then Allan, Margie, and then Ashley.

BRIAN KING: Thanks, Janis. While I think that I'll park this comment, but I think my colleagues to my right would be wise to run head on towards mere professorship. I wouldn't oppose considering the joint controller concept here. I think it would be a useful exercise to work this through. And to Ashley's point, to assume ICANN is the decision maker, a kind of centralized place, what does that look like? We're totally on board with

discussing that and kind of working that through, so we'd be happy to do that. Thanks.

GINA BARTLETT: I'm sorry, but how do you integrate that comment with what we just heard from at least Volker's point of view around the vulnerability that creates for the contracted parties? [inaudible] understand your comment in that context? [inaudible] connection.

BRIAN KING: Sure, [Gina.] I think we could spend a bit more time with the legal memo and kind of understand that concept a bit better and that rationale, I hope that helps to kind of explain the connection.

JANIS KARKLINS: Thank you. Stephanie was next.

STEPHANIE PERRIN: I just wanted to clarify some of these concepts of controllership. As Alan said, yesterday I said it's not where the data is, it's who calls the shots, who makes the decision. That does not mean that the people making the decisions should not be the ones closest to the actual registrant and the jurisdiction in which the data protection law might apply, partly because a lot of these disclosures are going to be governed by law that is not data protection law but administrative law, possibly criminal, [MLATs] kick in. We haven't even talked about transporter data flow,

but this is not something one can ignore as we create a model. It's a very real thing.

So that's why we call it local knowledge when you're making decisions about your public, your end user. The more local knowledge you have, the better the decision making is, in my humble opinion. So that leads you back to the registrar.

In terms of this ambiguity over whether ICANN is a data controller, a co-controller, a data processor, that's only stemming from the fact that they haven't made the decision. It was crystal clear as far as I'm concerned – and I believe the data protection authorities agreed with me – that back in the old days under the 2013 RAA where the contract said you shall provide this data and it shall be as follows, they're the controller. They called the shots. The registrars would be deaccredited as registrars if they didn't follow the rules, and that was followed up by enforcement action on accuracy and compliance. So hey, sounds like a controller, walks like a controller, quacks like one, is one. Right?

Now what we're talking about is ICANN making up its mind if it takes over. Like I keep saying, you can't outsource disclosure of data to a processor and turn your back on it. You've still got the liability. I see Alan nodding. Anyway, I just wanted to try and clarify those concepts. Thank you.

JANIS KARKLINS: Thank you. Alan, please.

ALAN GREENBERG: Thank you. Wasn't what I was going to say, but he follow-up to what Stephanie said, I spent a good part of the last 13 years of my life sitting in PDPs, making rules about gTLD process and how gTLDs are handled. There's no way ICANN can set all the rules or many of the rules and not be a controller. Yeah, we may be a co-controller, we may be the sole controller, we may be joint controllers, but there's no way we can not be a controller. It just doesn't make any sense. We write the rules.

So let's get that off the table. And I wish ICANN – I think I heard Göran say the same thing yesterday. So what I said before was following up on Ashley's statement that if indeed we are either the controller or a co-controller or a joint controller, if legally we can then decide which of the controllers – if there are multiple ones – make the decisions, then let us decide – that is ICANN.

I did not say the contracted parties can subcontract with ICANN to do it. That doesn't remove legal liability. I understand that completely. But if we decide through our joint contracts that exist that we are one of the controllers or the controller that makes the decisions, that is the premise I thought that Ashley was proposing.

JANIS KARKLINS: Clarify what you mean by we.

ALAN GREENBERG: I don't remember where I said "we" now.

JANIS KARKLINS: Where you said we are the controller.

ALAN GREENBERG: ICANN Org is the controller. I'm sorry. So it was not an issue as Volker implied that we're talking about outsourcing to ICANN. We're talking about ICANN as a controller or as the controller making the decision, and that's the question of, is that something that we can legally do or not?

JANIS KARKLINS: Thank you. Margie?

MARGIE MILAM: To follow up on some of the discussion, I think Volker, the memo – and when you have a chance to take a look at it, it actually cites from a case that says that the existence of the joint responsibility doesn't necessarily imply equal responsibility of the various operators that are involved in the processing of the data. On the contrary, those operators may be involved in different stages of that processing of data and to different degrees, so the level of responsibility of each of them must be assessed with regards to relevant circumstances.

So all we're really talking about is if you're assuming there is a joint controller and you're assigning the obligation to ICANN, then you're effectively doing that. You're just changing what your role is in the processing, and by doing so, reducing the liability. No one's saying h there's no liability, but the case law is saying that there's different levels of responsibility there. So I think we should take a look at that, and

maybe if you have questions, ask Bird & Bird as to what that means. But that seems to be what they're saying in the memo.

JANIS KARKLINS: Thank you. Ashley, please.

ASHLEY HEINEMAN: Thank you. Yeah, so I think we often heard different things when Göran speaks, and I think –

JANIS KARKLINS: He should be a lawyer.

ASHLEY HEINEMAN: I'm a Göran whisperer. I think I kind of sense what he really means as opposed to what he's actually saying. So what I heard is that he's not willing to take on liability risk. But what he's saying is that he's not in a position to indemnify. And I understand that.

I was involved in this little thing called the IANA stewardship transition, and there were sometimes calls to indemnify parties. That's just something you can't do. So I didn't take what he was saying as ICANN was not willing to take on this responsibility and take on liability risk.

So I think we just need to be very clear there, and I think building off of what Margie just said, by assigning responsibilities a certain way and being very clear as to the processing activities associated with those

responsibilities, we are in a good position. And I think this literally can make everybody's lives easier.

That does not mean that the contracted parties will have no risk. You will always have risk, but we just need to very clearly define what that is, and that's going to, I think, pertain to the processing responsibilities. So I think that's all I wanted to say. Thank you.

JANIS KARKLINS: Thank you, Ashley. Allan?

ALLAN WOODS: Thank you. I'm going to try and tackle the horrible thing which people don't like, the concept of a joint controller agreement. At the very basis and root of this joint controllership will have to be a joint controller agreement whereby we can assign who we believe reviewing the factual controller that we see it exactly as you read from the memo who has the responsibility in that area. And from that flows what we would at the end of the day, if something was to go awry, that we could turn and say, "Well, we believe that the responsibility lies with ICANN in this particular instance we're taking the decision."

Which is wonderful. However, the DPA then will come in and go, "Oh, no, you got that completely wrong. It's actually the registrar's fault because they should have been clearer in taking that data in the first place."

So again, the risk is hugely there for us all, and I think we just need to be exceptionally clear within the joint controller agreement, and that is a

level of agreement between the controllers as to where it is, but also that every single process, every single safeguard, everything that we're trying to define here from a privacy by design point of view has to be above board and we have to be genuinely of the belief that it is correct before we can accept that.

I think from the registry's point of view, and I'm assuming the registrar's point of view because I will say to my poor registrar colleagues that they're probably even more so in the firing line purely because they collect the data, they issue the data protection warnings to the registrant or the data subject.

We need to – I've lost my point. The point of the matter is the JCA is key, and we need to be very clear. Oh, that was it. I got it. we cannot accept any situation where our risk is increased for no real reason. And I don't want to say that this is not a real reason.

From this particular point of view, we are at this table not because we have to create the SSAD. It's not something that is envisaged under data protection legislation. We are creating the SSAD because we are trying to fix a problem which is make it more predictable, make it easier, make it more secure for people to get this, as opposed to what the law actually intends. And what the law actually intends is that we – I'm a controller, they're a controller, and if you want to get data which is under their control, you ask that controller and then they do it. That is the decentralized, every man for himself type model, which can be relied upon here as well. But we've all come to this table saying, "Let's try and make it easier. Let's try and make it more unified. Let's try and make it more predictable for everybody involved."

That is not something which the law requires. This is something that we're coming together as a policy to say, "Hey, registries, registrars, this is something you're going to have to do now in your contract, not because the law says it but because we are telling you you have to do that."

So in order to get this policy through, we cannot say "Well, we fully accept that we're just going to add another thing to our contract which increases our risk to an unacceptable level." So I need to be clear on that.

I'm not saying that we do not want to do this. That is where the reticence comes from – not reticence, our worry comes from, is that we have to do this properly in order not to attract further risk to ourselves. We do it right from the beginning so that the risk maintains the same and we have an easier way for you, a better way for us because obviously there's a mutual benefit there as well, but let's just do that. And I'm going to end there because I've got [inaudible] from Ashley and that's good.

JANIS KARKLINS: You see, that would be a correct statement if you were not at the table. You would be called in and said, "So this is what we decided, this is what you have to do." So the point is you're at the table, you're an integral part of the decision making process, and we are trying to design a system where every interest is taken into account.

ALLAN WOODS: But then we're back to this whole community versus Org. The community doesn't sign the contracts, Org signs the contracts. So I'm at this table because I frankly want to be here because I don't trust that if we're not at this table, that we get a position where we would be happy.

I'm here as a necessity. I enjoy being here and I love you all dearly, but it is somewhat, in a way, under duress. So I understand your point, but I firmly disagree with "I have a choice to be here." I'm here because I think I want to get the best for my constituency and for registries and registrars, and then for everybody else as well.

JANIS KARKLINS: Okay. Milton.

MILTON MUELLER: Yes. I thought we were focused on a very basic and important and simple choice; do we want ICANN or do we want registrars to be making the disclosure decision? It's very clear we have the standard division here, that there are people who want it to be registrars and there are people who want it to be ICANN.

My understanding – so we need to talk about that, why that division exists. My understanding of why people want it to be ICANN is that they think that that will be more uniform and more predictable, I guess, that they know where to go.

Now, I think I would propose a couple of answers to that. Number one, in terms of knowing where to go, I think if we standardize the system,

we can have a centralized clearinghouse for requests and still have the registrars making the decision.

Number two, if we set rules, for example it's not like registrars can just decide "Eh, I'm not going to respond to this." It is part of the policy, they're going to have to respond and probably within a certain time frame, and they might even be more efficient at that than ICANN Org given what we know about ICANN Org's ability to get responses out of data protection authorities. I won't go into that.

So I agree in some sense that ICANN, it is I guess simpler to have a single person making a decision than multiple parties, but if we have a uniform policy and procedures, I think a lot of that problem is overcome. And again, our concern is we want the decision to be made in a way that is most accountable to the data subject, and we view the registrars as being in that position the best.

JANIS KARKLINS: Following what Milton said, we're also talking about automated system. If majority of cases will be treated in an automated way, whether it makes much difference where the decision is made, at the ICANN Org level or registrar/registry level, because it will be made in automated way anyway and unified way anyway, following unified policy principles.

So that's a question to those who favor ICANN as the decision making body, controller. Matthew. No, I think you came after – Ashley, go ahead.

ASHLEY HEINEMAN: I'll keep it brief. I won't restate everything I said, but just also to note when it comes to this concern over whether or not individual DPAs are going to come after you, I thought that was the whole point of the Strawberry team question; they're asking very clearly if liability could be limited in a centralized model. And if we get an answer in the affirmative to that, my understanding is no single DPA can challenge that at that point because you have some guidance coming from the European data protection board.

So I just wanted to throw that out there, but it also goes the other way; if they come back in a negative to that, you have a different situation. But I just wanted to flag that that is something that's also in play.

JANIS KARKLINS: But my understanding from conversation yesterday was that another important element in that model that was presented by Göran was the decision will not be made at ICANN. Decision will be made outside ICANN.

CHRIS DISSPAIN: Janis, if I may. No, that's not an important element of the model, it's a choice. It's possible that the decision could be made in ICANN, it's possible the decision could be made outside of ICANN. It's not "This model only works if it's made outside of ICANN."

I think Göran was just saying it may be possible that you could have a situation where a condiment – I know, it's ridiculous – is acceptable and that that organization, whatever it may be, is not only prepared to

authorize or accredit but is also prepared to say “And the question is okay.”

But equally, it may not be possible and it may need to be done within ICANN.

JANIS KARKLINS: Thank you for clarifying that. Matthew, please.

MATHEW CROSSMAN: I really liked Ashley’s point about being precise about allocating responsibility versus indemnification. I think that is a really important point. I wanted to kind of put out there though – because I don't think we've talked about it at all yet – kind of why the lack of indemnity could be such a problem for contracted parties.

Even if we allocate responsibilities amongst ourselves for disclosing the data, there's nothing that prevents an individual data subject from pursuing a claim against either controller.

So even if we've allocated those responsibilities and we amongst ourselves have agreed that ICANN is responsible for the decision and we’re turning that responsibility over and we have a portion of that responsibility accordingly, we could still face actions from third parties that we would have to defend and we would not have an indemnification from ICANN for those third-party actions.

So I just want to put that out there as that is why I think the lack of indemnification tends to be a sticking point with contracted parties.

GINA BARTLETT: I know there's a queue but I want to frame a question to see – so I've just been charting on the board this isolated question, decision to disclose. What I hear that is established is that there is a joint controller and that there's a need for the responsibilities across the joint controllers for their agreement on what their responsibilities are, it needs to be very precise, but that the contracted parties cannot increase their risk and they anticipate that the DPAs are going to hold them ultimately liable. That's an assumption I hear coming through, which everyone may or may not agree upon because it may be contingent upon how you think that agreement is structured.

With the proposal for ICANN making the decision to disclose – because that's where we're narrowing down on – there's a sense that it reduces the risk of liability to the contracted parties and there's a consistency.

We've also heard from Milton that maybe the variables that are important with regard to consistency is to have a standardized clearinghouse and a timely response, which maybe that could be part of the contracted parties if they were making the decision to disclose. They might be able to adopt those policies that you all agree to to provide that consistency. So that might be replicable across whether ICANN is making the decision to disclose or the contracted parties.

So if you look at the contracted parties component, the pro that has been identified there is that they're most accountable to the data subject. I think that I've heard a number of people say that as one of the pros, and this whole question around ICANN's unable to indemnify –

which Matthew just spoke to again – is a real driver, and this question around from the contracted parties point of view that they really anticipate that liability will still ignorantly lie with them regardless of how precise the joint controller agreement is.

So that's a longwinded summary of what you've been talking about, but he question I have is a number of you have advocated early on – and I think it started with Ashley proposed it as a straw proposal – let's have ICANN make the decision to disclose.

So what I'd love to hear from some of you is I'm hearing from the contracted parties that they support the idea of the joint controller agreement, but they're feeling compelled that they need to make the decision to disclose. Maybe not. so I'd love to hear from others, how do you feel about that? How do you feel about the contracted parties being the ones who have the responsibility for the decision to disclose? And contracted parties, it looks like I didn't necessarily get that right because Allan's got his card up, but as you continue, it would be great to hear that side of how you feel about that, what's the pros and cons, what would you like to see.

ALLAN WOODS: It's not that we think that the liability – if the joint controller agreement is good enough and the process that we create is good, then the joint controller agreement will be fine and will properly stand up to scrutiny by the DPAs. So we don't think that a joint controller agreement in every situation will end with us being liable. We just need to make sure that we are happy with the entire process throughout.

JANIS KARKLINS: Okay, but then immediately the question is whether registrars agree with that and whether you consider that the joint controller agreement would be the sufficient insurance policy for you to accept that ICANN is making decisions and asking you to disclose data. So whether we can explore further that part, or your position is that no matter what is written in the controllership agreement, it will never be enough for you to feel comfortable. So that's the question. I'm not asking immediate answer, but just please think about it. I have Alan long waiting, and Hadia and Margie as well.

ALAN GREENBERG: Just a quick comment. I also heard what Ashely heard, that Göran was not willing to indemnify for 4% of Verisign's gross income, or GoDaddy or anyone else. But they were willing to take responsibility. However, Matt raised an interesting question of third-party claim. And it may well be that ICANN would be willing to indemnify you for third-party claims based on their approval to release the data. That's very different than indemnifying you for 4% of gross income. Thank you. It's a good point.

JANIS KARKLINS: Thank you. Hadia?

HADIA ELMINIAWI: Janis, you were asking about what other reasons would make ICANN a good party of disclosure. Other reasons would be auditing reasons and

introducing improvements to the process of decision making. And if you have one entity doing that, it's much easier.

Talking about liability, we have no certainties right now, but actually, the answer to the question that you've just put might actually bring us all to agreement. Thank you.

JANIS KARKLINS: Thank you. Margie, please.

MARGIE MILAM: I want to circle back to something that Thomas raised I think yesterday. If you go down this path where you have a joint controller agreement with the decision being made by ICANN, you might very well be in a situation where you can get insurance for the risk, should you be sued by a data subject, because the role that you're playing if that's the scenario, as we've discussed, would pose less risk than the party actually making the decision.

So I'm wondering if there's an ability to, as part of the system, make a recommendation that there be insurance for the contracted parties there and have – that's the kind of thing we could talk about in terms of, can the entire system fund insurance or self-insurance or something that alleviates that risk?

And Thomas, maybe you've thought about this before, but I know you mentioned it yesterday, and I think it's an interesting concept that we should also try to build into the system.

JANIS KARKLINS: So thank you. Stephanie, please.

STEPHANIE PERRIN: Thank you. I just wanted to point out that one of the things about starting with this concept of an SSAD – in other words, a big machine – is that our legal questions have been framed in a manner that sort of excludes much easier solutions. We don't need a big system to automate. I'm quite confident that the individual contracted parties can automate their responses where appropriate, but the reality is there's going to be quite a few responses that can never be automated.

So the idea that one party or another party is going to make a decision, ICANN might be in a joint controller relationship perfectly capable of making decisions on for instance rapid response malware attacks, and that could be staffed or that could be embedded. There are many ways to solve that particular problem. But they're never going to be able to deal with an individual consumer complaint in, I don't know, Mali or Barbados where they don't have the local knowledge of the law. That can't be automated.

So there's going to be offramps here. And the question of how these offramps, how many requests are going to be served through offramps, who would be the best, it's competency that a data protection authority's going to be looking at, and you can't outsource it to somebody who doesn't know what they're talking about when it comes to, say, a local consumer operating under data protection law in a country in Africa.

So we've got this gestalt that we're operating on as a centralized system, and we really need to knock that out of our heads, I think.

JANIS KARKLINS: Thank you, Stephanie. James, your turn.

JAMES BLADEL: Thanks. The conversation's moved on a little bit, but I just wanted to maybe just take a temperature of the room. I think what contracted parties – or at least I think registrars – are saying is that as long as we're on the hook for the consequences of making a decision, we have to reserve the right to make the decision. Is that a controversial thing to say? No? Okay. I just want to be clear, if a registrar or whoever says, "Boy, I stand to lose potential millions of dollars in fines, not to mention what my shareholders are going to do to me, but don't worry because I'll be fired anyway," if I get this wrong and somebody says, "Well, I disagree with you, ICANN should force you to do something against your ..."

Okay, I just want to be clear that we have a baseline that we all agree that people and organizations should not be forced into decisions that they believe represent true risk for them.

JANIS KARKLINS: My reading of your response is that no matter what is written in the joint controllership agreement, that will never be enough to comfort you that you would give up the decision making function.

JAMES BLADEL: So that's the next step, which I didn't want to take, but it does sound like Göran boxed us into that a little bit, which is that there's an unwillingness for ICANN Org to say, "If I tell you to make this decision, if I compel you to make a decision that you wouldn't have otherwise made, I still cannot indemnify you against any consequences," then it sounds like the joint controller framework starts to be fairly asymmetrical at that point and we just say, "Well, then we can't ..."

JANIS KARKLINS: No, I formulated a question following Allan's comment where he's saying if the joint controller agreement is detailed enough, precise enough and determines responsibilities in the process, so then that may be way to go.

So now you hear many around the table say that in their opinion, ICANN should be the one who determines to disclose or not to disclose. So you're saying initially, no, those who possess data need to be disclosed because responsibility is very heavy, lies on your shoulders. So I'm trying simply to find out whether there is any [inaudible] maneuver to reconcile basically t ow opposing opinions. So it is almost like in the anecdote where question is, who is the head of the family? The answer is obviously it's the man. And what's the role of the woman? The woman is a neck. And as we know, neck always turns the head.

GINA BARTLETT: I think that's a really bad analogy. [inaudible].

JAMES BLADEL: I just want to be clear that's not a trap, it's not a trick, I'm not trying to paint us into a corner. I'm just trying to understand I think what Allan is saying -and Allan, you weren't in the room, your name was being used in vain by me, sorry – is that, is a joint controller agreement enough to say that we are comfortable with ICANN making decision on our behalf that could result in massive fines and lawsuits? And no. Nothing is. It can't be.

JANIS KARKLINS: And I'm not trying to put you in a corner, I'm just asking whether that is something we could explore further. If not, then we're in a situation where you're saying no matter what happens, [inaudible] will make decision in every circumstance. Okay –

JAMES BLADEL: [inaudible]

JANIS KARKLINS: Yeah. But of course, you have.

JAMES BLADEL: I think what we're trying to say is, is there a scenario where we can transfer or escape the liability so that we can comfortably defer those questions [inaudible] and if what we're hearing, no, no, and also Göran, no, then I feel like we're being kind of boxed out.

JANIS KARKLINS: Again, I'm not trying to box you in every corner. I'm just trying to understand whether there is any maneuver possible in this respect. So I have Brian, then Chris.

BRIAN KING: Thank you, Janis. That actually feeds pretty well into the point that I was going to make and the direction I was going to go with this comment, is that – so I'm still answering the question that was posed earlier about the value of ICANN making the decision versus the contracted parties making the decision.

Milton mentioned earlier that knowing where to go is a benefit. I think that's a small point. More importantly though, reliability and infirmity and what we expect the response to be is the real benefit.

I think having ICANN make the decision addresses and fixes one of the real problems with the way that the decision making incentives are structured right now, and today, we're asking the contracted parties to give up data about their customers, and they're really incentivized not to do that. Because what could go right for them to do that? And we have a long list of what could go wrong as far as fines under GDPR, [cease processing] orders with no interest aligned to the disclosure of the data. It's a recipe for failure and it's failing now.

Whereas on the other hand if ICANN were responsible for making the decision, ICANN doesn't have an interest [in its customers,] in the registrants – when I say interest, I mean economic interest. If you're a

registrar who always discloses your data, you're not going to have a lot of registrants.

So I'd really like to be able to finish, please. On the other hand though, if ICANN is doing the disclosure, this policy addresses that, and I think writes the way the economic incentives should be. ICANN has an interest in the security, stability and resiliency of the DNS and therefore it can make a more objective decision than contracted parties are able to make.

JANIS KARKLINS: Thank you. Chris, please.

CHRIS DISSPAIN: Thank you, Janis. I want to try to give you a slightly different perspective on risk. Start with the presumption that the joint controllership is there, so ICANN and the registries and the registrars are joint controllers. If I understand it correctly, that means that each one of them is liable. The question I would ask you is whether you would prefer to have – [I'm sorry,] you also have to say there is a policy. So we've got a policy which has been endorsed and that says "This is the basis upon which you make the disclosures."

The question to consider is whether you think it's more risk to have ICANN build up a precedent of the way these queries are answered and have a reliable, continuous way of doing it that you can refer to and you can see, or whether it's less risky to have 375 registrars for one registry making 375 different decisions.

I accept completely the principle that you want to be in charge of your own destiny. I accept that totally. But I could, if I chose to, mouth what I would consider to be quite a strong argument by saying a single empowered decision maker is less risky than a myriad of people making decisions. It's certainly less risky, I would argue, to the registries. Registrars maybe different, I'm not sure.

And the second point I would make is from an ICANN point of view, if we are as liable as you are, then you're asking us to do precisely what you will not do, which is to take the risk without having any involvement in the decision.

So there is a conflict and there's a real difficulty in there to try and be sorted out. But from a risk perspective, I don't think it's fair to say simply the least risky way to be doing it is for the registrars to make the decision, because I'm not sure that that's actually true.

JANIS KARKLINS: I will propose the following. We have a number of plates up now, and I would – no, don't take them down. It was not the meaning of my proposal.

So I would take all plates which are up now to say, and then we would make a break for coffee but also for sort of group conversations just to try to digest what we heard in the room, and then see whether we can come up with something that everyone can say, yes, we can agree with that. Mark SV.

MARK SVANCAREK: When I was listening to James' concern, I was thinking that maybe I had misunderstood some of the earlier conversations because it didn't seem to me so cut and dry that you were being boxed in on all three sides. I thought Allan had said that a properly developed joint controller agreement would have resolved some of those issues. Pardon?

Okay, yeah. So when you were talking about your doomsday scenario, the three ways that you were being boxed in. I guess I hadn't heard the same thing in the room that necessarily all three of those things were converging on you like that. The problem that you put forward, clearly, and no one would agree to those things. It would be terrible and crazy.

I just wanted to reflect that I hadn't – at least I didn't think that I had heard that same convergence as you. So I just wanted to make that comment. Thanks.

JANIS KARKLINS: Thank you. Volker.

VOLKER GREIMANN: Yes. A couple of points resulting from the discussion. First to Brian, I think ICANN has a larger commercial interest in every single registration than registrars do, at least they make more money off every single registration than we do. So that's something I would like to contradict.

Second point, if we look at the concept of privacy by design, if we outsource the decision making process to ICANN, then we are already providing that private information of the registrant to a third party that

not necessarily has a need to receive that data because the data would be provided to ICANN to make that balancing test.

But ICANN still does not have the same complete picture that a registrar would have about the registrant because they didn't see the account data, they didn't see IP data. They have a lot of supplemental information that's available to us that we might look at as well when we make the balancing test. It's simply not available to ICANN or third parties. So the quality of the balancing test is likely to be lower than the party that actually holds the data and has collected the data in the first place makes that determination.

And the final point, every single contracted party that makes the test only has to be an expert in the data privacy laws that affect themselves. ICANN would have to be an expert in every single data privacy regime that's out there regardless of where it is, because they would have to apply the correct rules in every case of applicable jurisdiction that may be applicable in every single case, and that's a significant investment on the part of ICANN that I'm sure that can be done, but it's simply a consideration that may be worth considering when you make a suggestion like that.

JANIS KARKLINS: Thank you. Thomas?

THOMAS RICKERT: There's been a lot of talk about 4% of the annual turnover and that ICANN can't afford to indemnify other parties. Let me try to demystify

that point. I think we have been discussing it a couple of times over the last couple of months, but I won't give up. Humor alert, but you can also pay Ruth a little fortune to answer the question for you and then not believe her.

So you need to make a distinction between two attacks that can be launched. One is by the authorities. The authorities do fines. And if you have a joint controller scenario, the authorities will still only fine the wrongdoer. They will not fine all joint controllers. And that's where the 4% of the annual turnover are.

So the risk of a contracted party being sanctioned at that level if some third party, let's say it were ICANN, messes things up, is unrealistic. Where the joint and several liability kicks in is let's say an agreed data subject takes the joint controllers to court and is being granted damages by the court or that you have to pay for the legal fees for the court case. Then in that case – and that's the concept of joint and several liability – the agreed data subject can go after each of the joint controllers.

But then the joint controllers internally – and that's something that you would write up in a joint controller agreement – can go after – they can get indemnified internally, get recourse internally. If joint controller A does something wrong but B is gone after because that's the entity that's the most financially viable, then B can go to A and ask for recompensation.

And what you have then is the risk that your contracted party or joint controller might go bankrupt in the meantime. This is why I've suggested that we need a security fund to have some money parked

there in order to take that solvency risk away from the parties. But then again, we must not see the joint controller scenario as one agreement with thousands of parties, but you have little triangular relationships between ICANN, the individual registry, and then the individual registrar through whom the individual data is being collected.

So the risk is further reduced if you actually take it to this micro level. So maybe we should actually write these things up, but I think it doesn't do our discussion good that we're always afraid of these huge amounts while in practice the risk in my view is pretty manageable, particularly if you look at the European modesty in damages compared to other jurisdictions. And I'm not looking at Ashley now.

So I think let's be realistic and let's try to find pragmatic solutions and safeguards in order to protect the most vulnerable parts of this ecosystem against financial losses that they have not caused any wrongdoing.

JANIS KARKLINS: Thank you. Alan G.

ALAN GREENBERG: Thank you. Again, I'm going to harp on the fact that we hear different things from different people and one person's stating as fact – I mean, the fact that Thomas just said that it is only the party that made the decisions that is liable for the 4% changes the perspective, because if ICANN makes the decision, there is no liability other than from third parties on the other contracted party, and vice versa, the other way. if

that in fact is correct, then that's an important issue because we keep on raising liability issues.

And I put my hand up originally in response to James that I don't think anyone here is talking about you accepting liability for decisions you didn't make without reasonable indemnification.

So that's a given. If we assume it's ICANN going to make decisions, it's going to be because the Strawberry team gets an answer from the data protection board that, yeah, that does allow you to do that because of your joint controllership or unique controllership or whatever.

So I know everyone wants to protect their own turf, but let's not presume that the others around the table are malicious. No, you didn't say that, but the implication that someone around the table might want you to accept major risk where you didn't make the decision I think is a presumption of something that I don't think we need here.

UNIDENTIFIED MALE: I suspected that no one did. I just wanted us to get clarity on that as a starting point that we could all grab on to and agree on, and then move from there.

ALAN GREENBERG: I think we're all agreeing.

JANIS KARKLINS: Thank you. We have two further interventions, and then we break. Milton.

MILTON MUELLER: I want to thank Brian for being very direct. And sometimes when people are direct and honest about what's motivating their position, we realize that we are farther apart than we would have otherwise realized. But I think it really comes down in registrar versus ICANN, the uniformity issue as he indicated is kind of minor, and in my opinion overcomeable.

What it really comes down to is the perceived incentives of the party. So he sees the registrars wanting to guard the data of their customers, and so do I. And he wants to eliminate any incentive to protect the data of the customers, and I want to enforce it.

So we just have to realize that that's where we are. It's not like I'm saying he doesn't want anybody to protect data according to the law, but I think he believes that the registrars would be overly protective and I believe that ICANN would be underly protective and fundamentally unconcerned with the rights of the data subject and more concerned with appeasing a large interest who want access to that data.

So this is just a fundamental division, and we don't care if there's a joint liability agreement or joint controller agreement. If we feel that data subjects' rights are being violated, we're going to sue whoever we can, and we're going to sue whoever has the most responsibility and whoever we can get the strongest legal case against. That's just the way things are going to work out.

So I hope we can resolve this issue, but I don't see that having the registrars do it would fundamentally impede the interest of legitimate disclosers. I do believe the opposite is kind of true. I think one of the reasons people are pushing for ICANN is precisely for that reason.

JANIS KARKLINS: Thank you. Allan, you're the last one.

ALLAN WOODS: Thank you. It's always bad to be the last. First, obviously in my absence I missed a little bit, but to warn everybody, the toilet's on the third floor [because the ones that aren't open are the next door.]

Anyway, obviously, I just wanted to clear up – and I think Alan maybe – well, first things first, obviously Thomas said far clearer and with far more finesse than I ever could, and I'm really jealous because he's not a native English speaker. But I actually agree with everything he said, and I just want to clear up something that Alan just said there as well.

ICANN may be responsible in the JCA. However, if we accept a process or a policy that we know is not up to standard, then we're all liable. So it doesn't matter. And it's a factual thing that the DPAs [inaudible]. So I was not saying that – I would not drop my registrar colleagues in it. I'm saying that if, A, the JCA is in place and we properly coalesce the responsibilities, and B, we are all happy with the system and happy that there are supports and safeguards in place for whoever makes that decision – let's just say it was ICANN – if all the safeguards were right and proper and correct and we believe on a balance of probabilities that

they are legally sound, well, then it should be only ICANN who get fined in that instance for making that wrong decision. Should be.

I'm just saying that we can't get rid of that worry as well.

JANIS KARKLINS: Yeah, but we can work with that hypothesis, that if every piece as you said is in place and you are in agreement with whatever policy recommendations this team will come up and council and board will endorse, so then potentially, we can think of ICANN as a decision maker. But every condition needs to be aligned and you need to agree with that.

So I think that that may be an interesting takeaway from this conversation provided that you can agree with that. And again, I'm not pushing now for any answer, we're taking now a break, 20 minutes until half past, and if you want to chat among yourself – so that would be useful.

GINA BARTLETT: [inaudible].

JANIS KARKLINS: Yes, I think so, unless – sorry?

GINA BARTLETT: [inaudible].

JANIS KARKLINS: Yeah, we will stay on the subject after the break, and you will be first to talk. Okay? Thank you.

GINA BARTLETT: Hey, Fiona, can you ask those folks out there to come in, please? Thank you.

Okay, so what we're going to do next, we have a few more things we're going to try to cover before we break for the evening. We're going to pick back up with this decision to disclose. A couple people wanted to weigh in on that. But then we're going to ask you to go away, think about it more, talk with your groups and think about what would make it acceptable, how would you – to accept one of those, ICANN Org or the contracted parties to be the decision making, and be prepared to have a conversation about that either later tomorrow or in the future to find when that would happen.

So we're going to talk about that a little bit more, then we want to walk through the balancing test because we think that will be helpful just to walk people through that. Then we're going to try to go to building block L and talk about query policy, then I'll summarize what you'd agreed to today as far as the next steps, and then we'll agree on what we're going to talk about for tomorrow. So we'll walk you through that.

I just wanted to provide a gentle reminder that I've had a couple people come up to me in the break expressing frustration around people ascribing editorials for why people think about things. "Oh, so and so is

going to think that we're going to get better treatment because we have some kind of relationship or others don't believe this or they believe this because of that."

We just want to ask everybody to kind of put that in check and please just share your content and your idea and put to rest the editorials about ascribing motivation for why another party thinks something, believes something or is acting, and just share your ideas and points of view, alright? Points of view meaning content and substance rather than why people think something.

Okay, so I think we're going to pick back up on the decision to disclose. We'll go to Brian. Brian was waiting before the break. So we will go to Brian and a few more comments, and then we will probably check in and go to the balancing test. Brian, thanks for waiting.

BRIAN KING: Sure. Thanks, Gina. I wanted to kind of piggyback on Milton's point before. Milton mentioned that we wanted to remove the incentives to the contracted parties to protect the data. I think that was not quite what we intended with the comments, so I wanted to clarify that the current incentive structure is not resolving an access that works today. So the concept was that if we tried out a concept where ICANN is the decision maker, it removes that incentive structure that's resulting in a world where we're not getting reliable access today.

So that was the concept, and in the ICANN decision making world, while I think we prefer that as a change of pace because the contracted parties decision making world isn't working today, I think we're open

minded and we're willing and able to work in a concept where the contracted parties make the decision today. I think we'll definitely need more around how that might work and how we might be able to still get predictable access now that might be enforceable, but we're here to collaborate and be open minded about that. So if there's any constructive suggestions, we'd love to work with everybody on it. Thanks.

GINA BARTLETT: Thank you, Brian. Any other comments at this point on decision to disclose between the contracted parties or ICANN Org given all the considerations that have been put forth?

I did want to, Chris, put you on the spot. I touched on this in the hall, that there was some question and assumptions that they heard from Göran yesterday, the EPDP, that ICANN Org wasn't open to being the decider to disclosing. Could you clarify if the board has issued an agreement or if you think that can still be in the discussions and on the table for the group?

CHRIS DISSPAIN: Hi. Yeah. No, the board has not had a discussion about it. I think the way I would say it is this: I'm going to use WIPO as an example just because it's already been mentioned, so not necessarily meant to be specific.

I'm literally, as Janis would say, swallowing the microphone. It would be great, I think – leaving aside all of the things that none of this would be great for some people, but it would be great if you could find an

acceptable organization that was able to accredit – I may not use the right words. Accredit the people as being the right people, etc., and being subject matter experts [also able] to provide verification of the question. That would seem to me to be a good thing.

However, it's entirely possible that that will be impossible in some circumstances. And in those cases, then clearly, someone has to be the decider. And I do not believe that ICANN has said that it would not or could not be the decider. It's a matter for discussion. So I do not think that that is off the table. Thank you.

GINA BARTLETT: So it seems like today that there's – I don't want to overstep it, but a recognition that ICANN Org and the contracted parties will be joint controller. On the decision to disclose, there's two proposals. One is that it be the contracted parties and the other that it be ICANN Org. And some elements that have come clear to manage the pros and cons of which party is actually making the decision seems to be that there could be a standardized clearinghouse which provides consistency, whether it's the contracted parties or the ICANN Org, agreed upon timely response, and that there's this concept of maybe an insurance possible to alleviate some of the risk or some type of risk fund or some other type of variable, some other type of fund or ability to help manage some of those financial implications. Not that anybody's decided any of that, but those are options to consider regardless of who the parties are, who's making the decision.

Okay, I've got Alan G, Stephanie, and then we'll see if we can go to the balance tests.

ALAN GREENBERG: Thank you. I just wanted to point out that my understanding of what the Strawberry team was going to be hopefully getting some feedback from the data protection board is whether ICANN making the decision presumably as part of a joint controllership with appropriate contracts is something that they would agree is legitimate. if they come back and either don't answer or say "No damn way," then our decision is quite clear.

If they came back saying "Yeah, we can live with it," then we have to make a decision saying, "Do we all want to go that way or not?"

This discussion is really interesting, but it really is contingent on getting a definitive answer from them, which may or may not come.

GINA BARTLETT: Thanks, Alan. Stephanie?

STEPHANIE PERRIN: I've mentioned this before, and I would just like to throw it on the table as your third option. We're working on the concept of an independent data trust. That independent data trust would have a board. The registrars and ICANN and the registries would all be participants in that data trust. There would be data protection authorities, there would be consumer protection experts because that is a whole sphere of

expertise, and you're going to get a lot of independent requests from individuals and consumer organizations along that line. Bearing in mind the volume will go up because ICANN hasn't respected data protection law in the past, so there will be a new influx.

So that's the model that – and there would still probably be streams where it would automatically go to certain parties because it's noncontroversial. Thanks.

GINA BARTLETT: Great. I think we're going to move to walking through the balancing test, and I think the ask of you now, recognizing you're waiting to hear from the meeting that the Strawberry team is having, is for you to be talking amongst your constituents around what would make these options acceptable to you, what would have to be part of that, and to be thinking about that and be prepared to talk about that at a future meeting. Okay?

So, do you want to set this up, Marika, the balancing test, what we're going to do? Or Allan's going to walk us through.

ALLAN WOODS: I feel like I should proviso this and say this was something that I literally did in an hour, so maybe it was good work because I only spent an hour on it, but I'm happy to go through with you.

This was literally based off of how I approach doing my assessment. It was a practical application of how I thought – because I am the person who within Donuts gets these requests and looks at them. So I was to

apply a 6.1(f) – and I'd just like for the record to say I have never had to apply it since it began because I haven't gotten that actual request yet – this is the way that I've created the process for my company.

So there's three stages which you obviously can't see on the screen at the moment, but the first one is it is a preliminary assessment of the 6.1(f) itself. So I do not – and I cannot – process the data of the registrant until I know that there is a valid request in my mind. So I can't look and say, "Oh, I've got a request in for this domain. Let's have a look and see who the registrant is and go from there."

No, I have to actually look primarily first at the request and say, "is this valid enough for me then to say I actually have a reason to process the data for this request?" So the first step is establishing that.

The first one is obviously, who is the requestor? Who is making the request? Can I verify their identity, and do I need to take extra steps as to verifying that person's identity? And I think I mentioned that that potentially could be one element of where a very basic accreditation is because it verifies the identity of the person. That is great because it adds that first single step to the process. As I said, it's a subset of the policy work that we need to look at, and that's identity.

The next question that one has to look at then of course is for what reason, as is stated and not as is assumed. So again, I cannot supplant in my brain the reasons for a person requesting. A person can come to me and say "I have a trademark, I'm looking to request the data relating to this." And I have gotten those requests and I've gone back and said "Okay, I'm very happy that you have a trademark, but why do you need

the data?" Because they have not actually linked the two things together.

And I'm not looking at anybody in this room because I don't think it was anybody from this room. A much more small request that I've received. And it's literally you need to link it for me, I'm not going to assume that you have a reason for this request. So give us the data that we need in order to make this second assessment, that is, what are you using it for?

Necessity is a very important aspect, and if we do have that reason, we must look as to why you believe it is necessary to get this data in order to achieve that which you're stating is your request.

And again, taking from things such as – actually the Bird & Bird memos, because they've been wonderful for me for my internal – necessity is not absolute. It is not "You must definitely absolutely need this data in order to do it." It just must be reasonable in the circumstances of that request. Is it reasonable that you have gone through as much as possible before coming to me to contact that registrant? If you just need to send a cease and desist notice, have you gone through the registrar's portal to send it through to the registrant? Because in my mind, that is a necessity issue. If you haven't sent the request through to the registrant via the portal, then you should do that first, because it's a very clear lack of necessity for me to give you the name and e-mail address of that registrant when there is something that you can just achieve your purpose by sending that through the registrar registrant portal.

Now, if you've tried and you've not received a response in a certain amount of time, and you feel "I would like to be a little bit more forceful in that and I would like to send it through myself," well, then say that to us as the request. And I say us, I mean in this policy, what we should be looking at.

And again, give us that detail of the preliminary efforts that you have made so you establish the necessity of that particular point as to why you need to get that data and why that data needs to be disclosed.

And obviously, again, in that particular instance, all you need there is possibly just even the e-mail address. You don't even need to know a name at that point. It could be justifiable for the name at that point as well, but again, you need to give me that data, you need to tell me why you need it. So that's the second reason. I don't know how I got two lines in like ten minutes of talking.

And then, is the release of the data necessary to achieve the purpose as stated? I may have jumped ahead slightly, but that's exactly what I'm saying. Again, you have stated a purpose. Is the data that you requested and the reason you stated that you need that data, is it necessary to achieve the purpose that you have stated? So that's the preliminary.

If I can tick those three boxes first, it's only then that I move on to the second. Actually, there's one more. Sorry. Apologies. And that is, are the data elements requested limited and reasonable to achieve the purposes stated as well? Again, that's me going back to this idea that if I want to send a cease and desist, all I need is an e-mail address and

perhaps the name. You do not need to know the phone number, because you don't send a cease and desist via phone.

So again, it must be limited and reasonable to the purpose that you're stating, and it's an assessment on that.

So then at that point, if I have ticked those boxes that I believe there is a legitimate purpose of sorts here, that there is a limitation, I can link the reason for the request to the data which I have, well, then that's when I will make my second assessment, and that is, look at the actual data, because now I believe I have a legitimate purpose to look at that data for the potential to disclose.

Looking at that data then, the first question I ask in Donuts is, well, is it subject to the GDPR? And for me, that is a twofold test because one, is it a registrant who is A, is it a legal entity? And I will always ask that question first. And if it is a legal entity, then I'm happy to release because there is no personal data in that, unless of course there is personal data in that if it is a sole trader or something like that. Again, I've never had to make that decision, but that is one particular tick of that test.

The next then is, are they located within the European Union? Is it subject to GDPR? Are they located within California? Obviously, is the CCPA located as well? So I have to ask those questions. The information that is being looked at, is it protected under the GDPR? And I do make the assessment. If it is somebody in Azerbaijan, then I'm quite happy to say "That is somebody in Azerbaijan, I don't know of any protection that

would prevent me from doing that, therefore I'm safe to disclose at that point."

If it is somebody in the European Union, then we have a slight issue. Not issue, we just have to move it on to the next stage of the test. If as well the person is not within the EU, I need to then check for another thing, and then I need to look at the registrar, because if the registrar is a European registrar, then all data within that registrar is also subject to the GDPR and therefore I need to move on to the next stage, and that's the balancing test, because again, even though they're not within the European Union, I need to make sure that I apply the protections that apply to the data coming from that registrar.

There is a harder layer within that that, again, thankfully I've never had to deal with, but the question is if it is a registrar who I know have a whole rack of resellers that potentially are within the European Union, if that person is registered through that reseller, then it may very well be that they are subject to the GDPR, and I am not allowed to release that without moving to the balancing test. But I don't really know is the question of that. So there's a hole in the policy in this alone, because we need to figure out a way to figure out, is there a reseller involved in this?

And at times, it might be available or accessible via looking at things like nameservers, but again, there is some creative thought having to go into assessing these request. So that's one thing that we probably could put into that, is what is the interplay with a European reseller in that? And as we know, there r plenty European resellers out there and it's very hard to tell. So that's that particular one.

I say here, “Does the data contain personal data?” Have to ask that. If it does contain personal data, does the data originate within the EEA? And then if I'm happy – so at this point I may have already disclosed the data, quite happy to do that. Most of the time, a lot of these come from their privacy protection, and in that instance, I'm like, “Great, it’s a legal person and it’s also not in the European Union,” usually, so I would disclose that at that particular point.

Now, obviously, very disappointing for whoever’s requesting that data because it doesn’t help them greatly, but my counterpoint to that is if they’d just checked the WHOIS in the first place, they would have seen that. Well, in my case, every single one of them, [yes,] necessarily, but I take your point on that.

So the next one then is apply the balancing test. And I am not going to necessarily go through the balancing test because what's written here, I will put my hands up 100% and say were copy and pasted from the [city] Bird & Bird memo. And it’s the application of the [Regus] balancing test. But I will go through it very simply with you.

So the first one is the assessment of the impact. You need to put yourself in the place of the registrant in this particular instance and say, “If I was to release this data, what would be the material impact to that registrant in the case that has been sent and pointed out to me?”

Now, it’s a difficult one because I don't know what level that the European Union or the European Data Protection Board would assess that, so I have to kind of do it from a best case scenario or a common sense principle point of view. If I was to release this data, what would

be the effect to my registrant? Again, I'm lucky, I've not had to actually go through this process, but that is what the [Regus] test asks for at the beginning.

The next one then is the nature of the data. Again, the factor requires consideration of the level of sensitivity of the data as well as whether the data's already publicly available.

There are arguments on every side of whether or not the data is sensitive, but we must remember that we're not talking about sensitive data, we're just talking about the impact that this particular piece of data could have in the circumstances outlined in the request. And it really depends even on the requestor as to how sensitive that data might be in a particular in stance.

This is kind of the importance of the balancing test, and I think the [Regus] test is kind of important as well because on the front of – and I'm sure many people know of the [Regus] test and that was the opening of a car door to hit a tram, and the tram company wanted to sue the person who opened the car door, hit the tram, and they wanted the name of the person who opened the door in this taxi, but it transpired that the person who opened the door was a minor.

So in the general situation, it's probably releasable because they can get the name of that person, however, because it's a minor, you must take that into account in the balancing test, and in that particular instance, it probably would have failed because it was a minor and therefore there's another consideration on that specific case by case basis.

Now, I'm sure, Thomas, you probably have a much better in-depth understanding of that particular case but that was my kind of very general understanding of that.

And then the way the data's processed. So the manner in which data will be processed affects the balance of interest. Of particular relevance, the WP29 stated whether the data are publicly disclosed or otherwise made accessible to a large number of persons is an important consideration.

So obviously in this instance, we're not going to be releasing it to a large number of persons, but you can see in that line specially from the Article 29 work party why WHOIS as a concept was probably not the best thing, because it was to the world at large and that is a really difficult justification under this particular test.

The reasonable expectations of the data subject is another thing that was pointed out by Bird & Bird, and again, using the [Regus] test. And that of course is when I am giving my data to the data controller or to the data processor on behalf of the data controller, what do I reasonably expect is going to happen to my data?

And as a purist- and we can have many conversations about this – I give my data as a registrant to the registry in order to register a domain. I don't expect to be giving that data to everybody because they may claim to have a claim on that particular domain or they believe that I'm breaking a law in a particular jurisdiction. I am just giving my data to register that domain. So that is a concept. Again, that is up for

discussion. I'm not saying that's true or not, but it is something that is up for discussion.

And then the final is the status of the controller and the data subject. Again, the position of power – there's another one, there's an imbalance of authority that you need to consider. And in my mind, there's also an imbalance of authority between the requestor and the data subject as well in this balancing test.

So if I am a person – I won't give an example, there a really good example but I don't want to say it on the record to be honest because it's a real-life example. Okay, I will give this example: imagine that there was a company that sells bread. We're going to call them Kennedy. And it was a family-owned business and kennedy.family was the domain. And I am a Mr. Kennedy and I take that domain name, and I register that domain name for kennedy.family. But Kennedy is a company who sells this artisan bread, comes and says I want to know who this person is because that's my trademark and I want to take it from them.

Me as Mr. Kennedy is like "I'm going to get this notice from a large company saying 'This is my trademark, you've stolen it from me.'" [inaudible] that's what you say. But the imbalance there is that I need to consider whether or not in this particular instance I think the imbalance there is best served by disclosure, or should they just take this person to court? Because my process is not as well-known as the court's process. and to be perfectly honest, I think there was an imbalance there in that particular one because there's no malicious intent here and it might scare that person into just giving their domain away.

So I know, this is like – but this is a balancing test, these are the things you need to consider in a particular release, the consequences of me giving this data to this particular company and what might happen to my registrant.

Now, obviously it's an extreme case, but again, these are all part of the balancing test, everything from A to Z we have to consider on a case by case basis, and that's why we're so adamant when we talk about a case by case basis. You can't take into account nuanced ideas like this on an automated basis. And again, jumping forward – spoilers – on the new legal memo, that's kind of what they're saying as well. It is important that you take into account everything on that case by case basis.

So that was the result in mine, and I came up with these three things. Based on documented conclusions, if you believe that of all the three steps from the beginning, you can move to the next, you can release. If you see the balance is not favoring release, you need to respond to the requestor that no, all the data shall not be released, and as a key, provide a reason why you are not going to disclose this data, because again, the requestor should know if they can remedy any deficit in the requests that they have made.

So again, an open dialog between the requestor and the controller is kind of important here as well. And they might be able to remedy, or they might understand and move forward. and then of course, the requestor may re-request and remedy those issues raised. However, if the requestor – and this is kind of the sting of the tail which adds to the balancing test, which is continuously evolving in effect, if I am a requestor and I keep making the same request and I don't remedy, or I

try to remedy or I try to push it through, to me, that is again the power of the parties are being balanced away from disclosure because they're being unreasonable in their request.

So that's a very [whirlwind tour] of something which I've never had to actually – thankfully – apply, as I said, but that would be my thought process as I go through. So it's not a very easy test. That's just for one domain request. So I need to be very clear, as the controller in this – and this is the level of detail that I would request and I would expect, and that's why it's such a difficult thing. So, any questions on that particular monolog?

GINA BARTLETT: I had James, Ashley, Hadia and Greg.

JAMES BLADEL: I don't mean to pick on you, Allan, but this is a process specific to the model that you have as a registry, and it doesn't have a hook or a test in there to see if the registrar had also conducted a similar test or if the requestor had exhausted that avenue first. It's completely independent of any other test that might be going on.

ALLAN WOODS: Yeah.

JAMES BLADEL: Okay.

GINA BARTLETT: Ashley?

ASHLEY HEINEMAN: Thank you. That was really interesting, to kind of play through. Very educational actually. One thing I wanted to note – and I'm sure it's abundantly obvious to everyone – I was not ware of the [Regus] approach, but what's really clear is that it's very subjective, and I don't know if that's something we should consider in our policy, if there's any way to make it more objective. I'm not sure, but I would assume that if this [Regus] approach is that that's well known, that maybe others have found way to make it more objective.

My other point is that – and I think to consider it a policy thing, the example you gave of people possibly just continuing to make being unreasonable in their requests, and like to point also back to our Freedom of Information Act where we also have in place guidelines for basically putting them on the bad list, so it would have to be objective as well but it would also, I think, be beneficial to a system that [inaudible] who is abusing it that they can be put to the side. So that might be another policy consideration.

GINA BARTLETT: Hadia. Oh, okay.

ALLAN WOODS: I completely agree, and I think that's actually really helpful. I think the difference here is between the SSAD and how I would approach it as an individual controller, because as an individual controller, it's up to me to decide at what level I'm going to apply that test, and if the requestor has an issue with that, they take it up with the DPA. But from the SSAD, we have to think of that more objectivity level, and I think actually [Matt] was talking specifically about the FOIA as being an interesting model to look at, and I think that's a good point.

GINA BARTLETT: Hadia?

HADIA ELMINIAWI: Thank you for presenting this to us, and I have one simple question. How much time does this whole process take from the time you get first request until you reach the final decision of whether to actually disclose or not?

And just you were talking about items like does the data subject for example expect their data to be processed in this manner, and then I guess this could be part of your policy notice, that you would inform your data subjects about the expectations of how their data could be processed.

And to James' point, I think he did ask if you did check if the requestor did go to the registry before or not, right?

ALLAN WOODS: [inaudible].

HADIA ELMINIAWI: Registrant. And why don't you do that step?

ALLAN WOODS: I'll answer that one first. My gut instinct is because I just didn't think about it. It never occurred to me as being a step. But also, I am a controller. I need to take it on the merits as they're presented to me. It could be a very important thing, but at the end of the day, I don't think it's probably a necessary check. It's a hard one, I would have to think about it.

If the person has made a request up and down the country for this, it might be a consideration but it might not. Again, it depends on the circumstances of the individual case. And I'd forgotten your first point. I'm so sorry.

HADIA ELMINIAWI: [inaudible].

ALLAN WOODS: Oh, yes. So the response to that is that awful of, "How long is a piece of string?" because it really depends on what the request is. So if I get everything in that initial request, it might be a very straightforward review. But if I need to check every single step along that line before I

can make a decision, and it depends on how quickly somebody gets back to me, it depends on my own time, it could take longer.

It takes as long as it takes to do that, but it could take a while and it could be a long tail. [Often] it could take days or weeks, but not because I'm delaying, just because I'm following a process.

GINA BARTLETT: Okay, I've got Greg, Dan, Brian, Milton, Matthew, Stephanie, Alex and Georgios. Greg.

GREG AARON: So on average – you couldn't answer that question?

ALLAN WOODS: [inaudible].

GREG AARON: Well, her question was how long does it take to evaluate, get an answer back. So my question is, on average in your experience, how long does it take for you to evaluate a response?

GINA BARTLETT: It sounds like Brian has an answer for that.

BRIAN KING: Yeah. Sorry to jump queue. I can answer that, not as to Allan but as to the hundreds of requests that MarkMonitor sends to registrars. When we get a real life response, like either the data or "Hey, can you clarify something?" We usually get that in two days and then the average of when we're ignored or nothing is increasing every day. It's usually two days.

GINA BARTLETT: Okay. Did you have another comment, Greg?

GREG AARON: Yes. So Allan, one of the tests is the reasonable expectations of the data subject. All of the registration agreements that I've read tell the registrant that they can expect that their data might be disclosed under a set of circumstances. If that's in an agreement, does that cover this need?

ALLAN WOODS: To be flippant about it, just because it's in the contract doesn't mean it's going to be legal. Ultimately, I still would have to go through the test, and if in the circumstances of that particular one, it doesn't meet the test, then no is the answer. Just because it's in that agreement will not mean that that is good enough notice for that person, to be honest.

GREG AARON: I'd like to learn more about that some other time. When you're balancing the impacts between the parties, there are two parties at

issue. So how do you deal with the interests of the requestor? Because the key of the balancing is the requestor has a stronger need for the data, or a stronger justification, whatever you want to call it.

ALLAN WOODS: God, I'm sorry, I'm literally going on a flippancy. The requestor is not my data subject. I'm here to look after the rights of the data subject. It's up to you to assess and to follow that through. If you're not happy with my response, then you must take that to the DPA.

GREG AARON: Well, I'm trying to understand that – I know what the law says, which is you take both sides into account and you have to make a determination about which side has tipped, right? So it sounds like a very subjective thing, but what I also hear you saying is you have a conservative view that's going to favor your data subject. Is that fair to say?

ALLAN WOODS: I think it's fair to say that every single data controller out there in the absence of having guidance or a court case on this will have to take the conservative view because we don't know for certain. We don't have to take the obtuse view, but it should be erring on the side of caution at this point.

GINA BARTLETT: Okay. Dan. Thanks.

DAN HALLORAN: Thank you, Allan. I want to echo what everyone else is saying, thank you for the document and then walking us through it. I think it's very clear you've thought this through a lot and you're applying it very carefully, and we can all only hope that all of the other 2000-something contracted parties all have someone as conscientious and qualified as you doing this test.

I'm not sure that's true though, unfortunately. And one thing, picking up on something James I think was hinting at, is if we think it's true we're joint controller, ICANN, the registrars and you, we're all kind of depending on you to make that test right because if you mess up, sounds like we might be jointly and severally reliable. [inaudible] that's where James was going. Thanks.

ALLAN WOODS: Just on that, I actually don't agree with you on that one, because I'm doing that – you have no – I used the word [for Chris earlier] and I thought it worked - factual influence over my decision. In that one, I'm acting a controller in that instance. I'm not asking ICANN's permission, ICANN is not making me release that. I'm working as a controller in my own right. And any DPA who would be reviewing that will say, "Well, is this decision forced upon you? Is this particular path forced upon you by anybody else?"

And it's like, no, this was my decision, my policy and my response as a controller in this instance.

Now, of course – I'm sorry, I'm just going to call out [inaudible] room, if this was a joint controller agreement and the SSAD was not a thing, that would be marked out very clearly in the joint controller agreement saying when you get a data disclosure request in such a manner, then whoever responds to that responds of their own [bat,] and I think that could be one of those things that we work into. But that's part and parcel, and that would also be told in the additional document which is necessary, which is the condensed version of the roles and responsibilities that would be given to the data subject to the registrant upon registration. It's that statement of joint controllership that we give to them.

DAN HALLORAN: Okay, I just want to understand [inaudible] if the registrar collects that data from the registrant, passes it on to you as the registry and now you the registry are deciding whether to disclose that to a third party, the extent to which the registrar might still be on the hook or ICANN Org who have a contract with you, my understanding from the discussions earlier was that the joint controllership concept is broader and we're all on the hook for all these processing [inaudible].

ALLAN WOODS: So the difference there is that in the actual way that it's set up at the moment – and myself and, say, James, we have a data processing agreement in place, and people know, the registrant knows that the data will be sent to the registry because that is part and parcel of the process.

however, the request will be made of me and therefore it would still be limited to me in that particular instance as the controller, and again, the factual influence of GoDaddy in that particular instance would be zero. And again, the DPA while reviewing that would say, "Well, yeah, they're not on the line for that at all," because factually and legally, it is my decision and only my decision. Even though we're joint controllers, in my view, it would be that.

DAN HALLORAN: Okay. Thank you for that. My other question is it seems like you have the idea that every time a company's going to do a 6.1(f) test, it has to do an individual balancing test for every processing activity and that you couldn't, let's say, pre-decide, like if I get requests from these kind of people for this kind of data for this kind of jurisdiction, it's okay to release that. You have to individually look at every request with your own eyes and make that decision on every 6.1(f) test?

ALLAN WOODS: It's a pretty hefty question, but generally speaking, yes, and thank you whoever [kept that document up and did put the reference in,] because Skynet isn't a thing yet.

Yeah, an eyes on would need to be done. And if I was to put these buckets in, they would be as a guide to me, but I would still need to be able to prove to a DPA upon a complaint that I did take an actual meaningful look at the individual circumstances of that request.

DAN HALLORAN: Sorry, last thing. I'm trying to understand if that would mean every time any company anywhere is going to use 6.1(f) for any processing, it has to weigh every single time, let's say, we relied on 6.1(f) to print out this name badge with Chris' name on it, do we have to balance, "Okay, Chris' we can print. Okay, León, can we print his name badge? Yes or no? Well, let's see, León ..."

Or can we just say, ["Hey, if you're interested in name badges,] you can raise your hand, 6.1(f), we're going to print all your name badges, it's a legitimate interest." Or do we have to do the test for every single person for every single print job?

I'm sorry, I'm not trying to put you on the spot. [inaudible] things I'm wondering and maybe we could learn more about together.

UNIDENTIFIED MALE: I've been thinking about this quite a bit, and I think we need to clarify what we mean by "Can this be standardized?" And I think in scenarios where you have exactly the same parameters where you will do exactly the same tests, you can apply the result of the balancing test for multiple requests.

Let's say there is a security researcher who is doing an analysis of certain incidents and you know the data is not going to be passed on, it's just for analysis by the researcher, that it's not being used to publicize that information, what have you. So you know the parameters, then it's safe to say that whenever the researcher approaches you with the same type of request, that you then can greenlight it; right?

While if, let's say you have – and this is what Bird & Bird alludes to – law enforcement requests from law enforcement authorities outside the EU where you need to do a 6.1(f), there it becomes extremely difficult because then you need to look at what is the law enforcement authority, what is the type of crime they're investigating, what are the potential sanctions involved with that? Is there a fair trial in the country of origin?

Because if you then apply standard tests, that might be to maybe just financial fine in one jurisdiction, but it might be capital punishment in another jurisdiction. So you need to be very careful about what's at stake for the data subject, and those things I guess don't offer themselves for any sort of standardizing or semi-automated processing.

So I think when embarking on this exercise, I would have hoped that we find commonalities in cases that are prone to it, but not all cases are prone to it. As I call it, a prefabricated balancing test.

GINA BARTLETT: Can I go on? Brian, thanks for waiting.

BRIAN KING: Sure. I really enjoyed this conversation. I really appreciate Allan for walking us through. This was really helpful. If anybody wants to take a look at another one of these, MarkMonitor's internal process for reviewing these requests and deciding whether to produce the data or not, it's on our website and I can send everybody a PDF if you'd like me to do that, if that'd be helpful to inform the discussions.

One point that Dan made, I wanted to think about. I'm not so sure that we are operating in the vacuum that we think we might be, and there might be some joint controller arrangement anyway. And the thing that makes me think about that is the temp spec requires us to – I don't want to [inaudible] contracted parties [inaudible] conversation – requires you to review and make the balancing test in those cases, and then that was also adopted in the phase one policy.

So even though you're kind of doing it yourself, the ICANN policy that's going to become your contract with ICANN does require you to do that and to do that balancing, so there might be a joint controller scenario, whether we intended to have one or not in that case. So I'd like for us to chew on that a little bit.

ALLAN WOODS: Bluntly, that's our fault. Maybe we shouldn't have done that.

GINA BARTLETT: Okay, Milton.

MILTON MUELLER: Thank you, Allan, for walking us through that. I appreciate the care that you're taking, at least in theory. And in fact, that's my question, is about you insisted several times that you never have actually done this. I'm just curious as to why not, because you don't get requests that are based on 6.1(f), or you have a different process for handling them? Why has this never happened before?

ALLAN WOODS: Simply because since the GDPR came into being, I have had 101 requests, and going through this process for me, I have never had to apply the balancing test because it's either – the vast majority of them, I had to deny many of them because they just weren't requests for disclosure at all, or they just have not been European data, because most of them – 90% of them – have been privacy protected, so review of our WHOIS will show that they've been privacy protected.

MILTON MUELLER: So [I think that's] relevant data in the sense that this is what, four or five months, almost a year of activity and you've gotten 101 requests and not one of them was a 6.1(f) one which you had to conduct the balancing test. So when we're talking about the scalability of your careful review process, I think that needs to be taken into account.

GINA BARTLETT: Thanks, Milton. I've got Mathew, Stephanie, Alex and then Georgios, and then we're going to do a jetlag stretch.

MATTHEW CROSSMAN: Yeah. Hey. I just wanted to ask you about kind of the – at the end of this, you talk about you need to document your conclusion and then you make a decision based on those conclusions. And recognizing that you haven't actually performed this yet, what's the level of detail necessary in documenting those conclusions? Is it you are just going to document the outcome of the balancing, or are you documenting facts

under each individual piece to the test? Because I think that's going to be important when we start talking about places where we can standardize or have some sort of automatic process. We're going to have to think about how we document those processes as well. so I'd just be curious to hear how you approach that.

ALLAN WOODS: Yeah, absolutely great question. In theory, I would document everything. I would document my thought process. And again – I can't think of the exact article, but it is that you have to show compliance, not just be complaint. That is the underlying theory of the GDPR. If the DPA comes knocking, me saying "I released this on this date but I did go through the balancing test" will not suffice. We'll need to say, "What questions did you ask? What were the answers to the questions, and why ultimately do you believe it was the right thing to release that data in that instance?"

And they might go, "Yeah, great, thanks very much" and move on, or they might go, "No, that was deficient." But at least I have the information as to why, "I see where you made your error, and don't do it again," as opposed to "I'm just going to fine you because that was awful."

GINA BARTLETT: Can we keep going, Matthew? Yeah. Stephanie?

STEPHANIE PERRIN: Thanks. I wanted to make three points. First of all, I really appreciated the way you walked us through this balancing test, Allan, very useful. One of the reasons we'll miss Buttarelli is that he was extremely eloquent to both the purpose of data protection being to recalibrate that balance between the rights of the individual and an information society where they're totally disempowered. So that's fundamental to the balancing test, figuring out that power relationship.

Secondly, in terms of automation, I hate to keep beating this horse, but if we come up with procedures and templates for certain types of requests, we can automate that so that it doesn't actually show up on your desk. If they haven't gone through – I would call it in our regime exhausting their administrative remedies, you referred to, well, have they used the portal?

And forgive me, I'm not a geek here, but I presume you can feed them a token when they use the portal and then they show up with their template, with their token, saying "Hey, we've done everything," because the actual requesting somebody's personal information from a separate entity is a nuclear option. You're not supposed to go there first. So we're breaking a pattern here where they always went to WHOIS first.

And if I remember – oh, yes, frivolous and vexatious. Again, there's a way to figure out the frivolous and vexatious requests, and that's what we call them in our jurisdiction. And boot those out of the system as well. Their remedy, as you say, is to go to the DPA and complain. Thanks.

GINA BARTLETT: Alex, thanks for waiting.

ALEX DEACON: Thanks, and thanks, Alan, for walking us through that. I just want to make three points. One thing that occurred to me as you went through this, epically in your pre-analysis, it's important that as we think about the system or the policy that will support this system, we make sure that all the data necessary for anyone or anything to make that determination could be conveyed in the request.

And I know we have policy principles and building blocks for the contents of a request and the format of the request and the completeness of the request, and I think that's important, we just need to make sure we don't miss anything there.

It seems to me – and I think Stephanie may have stole my thunder a little bit – that in a system, you can automate the completeness check. So if a requestor sends a malformatted, incomplete form, it will never get into your queue, they will get a response that says, "Sorry, try again." That seems helpful to me, and that would save you guys some work. Not all of it, but some. So I think that's worth thinking about.

You mentioned privacy protection a few times, and I kind of behind the scenes said that it's not always the case that it's clear when a privacy proxy is in use, and you said for Donuts, it is. I think in terms of predictability, we need to make sure that any policy that we create ensures that when anyone asks for this data, it doesn't depend on how

the contracted party has implemented it. There should never be a situation where it works for you but doesn't work for others.

So I think that was something else that came to mind, and we have this recommendation 14 in phase one that talks about privacy proxy and how you handle those. We need to make sure that that doesn't get forgotten or somehow added into whatever policy that we work on for phase two.

And then the last thing that you said that I thought was interesting and I just wanted to comment on was that you will always reply with a reason why things didn't fail. In other processes at ICANN and elsewhere, sometimes we just get a response that says, "Your case has been closed," and we don't know why. So what will happen there is that we will try again and we haven't learned nothing. There's not a positive or negative feedback loop there for us.

So I think it's very important in whatever system we develop here, whatever policy is behind it, that there is a clear indication as to why something failed. So we learn and we don't continue to bug you guys with requests that are not malformed in this case but just failed for a different reason.

And then lastly on the vexatious and frivolous, I think having a credential that kind of identifies an individual in the whole discussion that we've had around accreditation will kind of help minimize the frivolous and vexatious requests because we're going to know what they are and there's going to be hopefully a code of conduct behind it.

So I think there's a solution to those, which means less of those frivolous and vexatious requests will end up in your queue. Thanks.

GEORGIOS TSELENTIS: Thank you, Allan. Being last in the queue, I think many of the points I wanted to make were touched, and basically, the point I wanted to make was about the possible automation. Now, if this scales up – we are talking about a hypothetical model that you will receive many of those requests – can you identify the parts of the process that probably having a memory in the system would – and could from the requestor's side, the type of the request could be slowly building to something that would create an automated system that is more efficient for you also to deal with those requests, but also for the requestor if they have to repeat so many – if they have similar requests not to get to start from scratch every time?

ALLAN WOODS: Obviously, it would be so much easier for me if my system – which is my brain – learned with each and every thing. I think this probably touches on what Thomas was talking about. You can recognize certain patterns, and I think things like a particular requestor could over time build trust in effect that certain elements of their request can be taken at a much higher level because they have not abused the system as far as we know, obviously.

The thing is, how, again, when you're being judged on the final day by the data protection authority, will you be able to stand up to the scrutiny and them saying, "Well, why did you believe?" And you say,

"Well, we've had 300 requests from this particular person before and have never had a problem," they'll be like, "Well, are you sure ..."

Again, what are your safeguards built in? Why did you add this together? Ultimately, at the end of the day, I think, yeah, there might be some preliminary ones that may be put into the system. The system could learn to accept it more readily or might be a higher trust level.

I'm not the engineer or the be all and end all here, but I still think when it comes to 6.1(f), there is an eyes-on point where you need to – even if it's a trusted person – assess whether or not in this particular instance the balance is in favor of disclosure. And again, I think that's going to Stephanie's point about regaining that equality or regaining that balance of the rights of the registrant or the data subject in that particular instance.

GINA BARTLETT: Thank you, Allan Woods, and everyone for all of those great insightful questions to help us understand how this balancing test is working out for you, but for others as well.

okay, we have one hour left to go. Does everybody want to stand up and just take a stretch? Not leave, you're not allowed to leave. Have a stretch. One more building block today. Yeah, the shoulder massage, right? Margie is trying to leave.

Okay. So we're going to go to Marika, and Marika is going to queue up for us building block L on the query policy, and there were some comments around that from all of you. So we thought we would

potentially resolve those comments or identify what you need to discuss on this to potentially take that off your agenda for the rest of the meeting. So I'll pass it to Marika.

MARIKA KONINGS: Thanks, Gina. It's actually both building block I and L, just to make sure that people understand that the query policy is actually covered twice in the zero draft, once addressing the entity disclosing the data and then also looking at the SSAD itself.

So I think the information that is in there is taken from the review of the use cases by the groups. I think we already flagged there were some comments already in there that were left over from the use cases or kind of action items that were assigned. I think for example, there was a reference to abusive nature. A suggestion was made that it might be helpful to provide some specific examples as to what is considered abusive.

There was also actually still an action item for Marc A and Brian to work on potential rewording of point B. I don't know if you maybe recall that. I think it was the discussions in Marrakech. So again, that may be something that needs to be reviewed. It talks as well about the response should not include more data than requested by the requestor.

A point that several people commented on, whether the response should include public data elements related to the domain name registration. I think that's where some have suggested that that might

not be appropriate, and others I think have asked the question, well, why not? What's the issue here?

And again, this notion I think that has been discussed before that a request must be received for each domain name registration for which nonpublic registration is requested, and each such request must be examined on its own merits.

Some have suggested – and again, in their comments that maybe this needs to be further discussed after the entity disclosing the data is identified. We've had some preliminary conversations already around that. consider as well what happens if a person breaches the terms of service. Are they then prevented from being in receipt of any kind of disclosure?

There were some questions as well how point B could be enforced, and a suggestion that it may be worth considering simplifying and merging point A and B. Again, what I just noted as well, this notion of only including elements requested, should that prevent inclusion of public data elements – and again, maybe a question of discussing, is it really "it should not" include public data elements and must not? It could include, or it should or must include public data elements.

Again, I think several asked the question, what would be the [inaudible] the issue of also including that with the request as it is publicly available to facilitate requests by having all the data in one place.

There was also a comment that this might be a potential conflict with policy principle 11. I would actually need to check back which one that is. I think someone also suggested that adding each request should be

examined either manually or programmatically on its own merits, it should be called out.

And another question that was flagged, whether the query policy should also include the ability to submit multiple requests if linked to the purpose cited.

There's a second part to the query policy in the zero draft that focuses more on the SSAD and what requirements should be in place for that. Again, this comes, I think, copy and paste I believe from the first use case we reviewed, and I thought that at that point, there was general agreement around at least the concept in here, and I know there was some rewording that happened as a result of that review, so I think that was currently written as kind of a must, unless otherwise required or permitted, not allow bulk access, wildcard requests or reverse lookups, nor search capabilities. And I think that specific bullet was the source of most of the comments received in this regard where I think some indicated that it should not be allowed and you shouldn't even have the "unless otherwise required or permitted" part in there, while others I think suggested that that should be open for discussion and consideration.

And I think some also pointed out that how this eventually may end up looking is also dependent on what SSAD actually is and what it looks like. So I think that's in a nutshell what is in there and the input that was received, so I think it would be helpful to get some preliminary input on especially the comments, how can those be resolved for some of the open items that may still need to be worked on. And again, is there anything else missing as well? Because I think the input is mainly

focused on what is there, but are there other aspects or elements that should be considered and added to this building block?

JANIS KARKLINS: Thank you, Marika. I would suggest that we start with the building block L that is currently now on the screen, and see whether we are in agreement with those four bullet points that are formulated based on the use cases, because clearly, at the beginning of the process, I remember a few months ago, I had a feeling that we're in agreement that things like what I mentioned in subpoint A, bulk access, reverse lookup would not be any more acceptable.

And then the last use cases, there were already some incautions or some question, some team members questioned whether that was really the case and whether we could not use reverse lookups.

So it seems that there was kind of a shift of understanding, at least in minds of some members, and I would suggest that we start by thrashing out those topics and try to see whether we can close them completely and not to come back to them, nail down our common understanding.

Georgios – no. Milton, your plate is on this topic. Please go ahead.

MILTON MUELLER: Yes. We very much did in our very first use case have a discussion about bulk access, wildcard requests, reverse lookups, Boolean search, and it was agreed that that was not going to be allowable.

Now, the only thing I saw – I didn't see any discussion that reversed that. What I saw was a particular constituency submitted a use case at the last minute that basically asked for that. The fact that they asked for that doesn't mean that anybody agreed that that was acceptable, and I would submit that it's still not.

I'm particularly curious about the word "required" in there. Under what circumstances would any of this be required, and required by whom? We know some constituencies want it, but I think all of the legal advice we got, even going back before the temp spec, made it clear that that kind of activity would not be legal. So I would hope that we would just get rid of that language.

MARIKA KONINGS: Maybe just to clarify, I think the "required," at least as I recall from the discussion, there may be a situation where a contracted party in their renegotiation of their agreement would have a requirement for one of the – this may be very hypothetical, but I think that was where the kind of "required" would come from. And if through some other policy decision that's made in another context or through contractual negotiations, tree might be change in the circumstances that that would not prevent that requirement from being implemented. I think that's where the "required" comes from.

MILTON MUELLER: [Could someone from the contracted parties] speak to that?

JANIS KARKLINS: Okay, let's clarify that particular question. Volker.

VOLKER GREIMANN: Yes. For registrars, this is certainly not a thing, but I'm aware of certain registries that have agreed or have put into their PICs certain requirements with regard to capabilities that match these requirements. So some registries are offering reverse search, wildcard maybe, I don't know, but something along those lines. It's permissible in some gTLD registries.

JANIS KARKLINS: Milton, are you satisfied with that answer?

MILTON MUELLER: Yeah. I should have known that you could blame it on evil PICs. [inaudible].

JANIS KARKLINS: Margie, please.

MARGIE MILAM: I believe that the BC input came in early, it didn't come at the last minute. When we went through the use cases previously, I was under the impression that we were going to go through all the use cases and we'd have the time and place to make our case for it. So none of this is last-minute, none of this is new.

I understand there's concerns about some of this. I think the part that I'm probably okay with is not allowing bulk access in the sense of what used to be the old bulk [inaudible] if you remember in the old days, you could pay a fee and get the entire database. That's not what we were talking about.

What we were talking about in our use case was the ability to search via contact fields, and that's consistent with what was done before and is needed to be able to correlate domain names that could be related to the same registrant. We used that both for cybersecurity-related incidents, and I think the SSAC paper may have even talked about some of that. And you also do it for correlation in order to identify the domain names that you're going to bring a UDRP case against, and that's an ICANN policy. So that's what we're talking about here, is the ability to make request related to a specific contact field to identify other domain names that may be linked to that particular contact field.

JANIS KARKLINS: Okay. T y. Brain, please.

BRIAN KING: Thanks, Janis. I would clarify one thing. That language and those requirements in A are not in the PICs. They're in specification 4 of the registry agreement, section 1.10. It's the registry's option, but if the registry opts to do that, then these are the requirements. So that's where that came from.

With that said, I don't know what the –the repeated prohibition on bulk access as like a thing that used to be a thing does for us, so we could really lose that whole A if that makes everybody more comfortable with these requirements. In fact, I think we suggested that in our input to the zero draft just to strike all bullet A if that helps folks to live with this. Thinks.

JANIS KARKLINS: Thank you. There is a proposal to strike subpoint A completely. Whether that is something we can agree. Stephanie.

STEPHANIE PERRIN: Thank you. I just wanted to point out – not to put Dan on the spot as ICANN's privacy officer, but just because something's in a registry contract doesn't mean it's compliant with GDPR, and all of ICANN's previous policy decisions need to be reviewed in the light of GDPR. Otherwise, they're going to be getting complaints about what's going on. Thanks.

JANIS KARKLINS: So Dan should take note on that. Volker, please.

VOLKER GREIMANN: Yes. Just one slight note. I have received requests with wildcards and reverse lookup kind of requests from law enforcement as part of investigation into certain people, certain actions that they have done, and I have granted those requests because I felt that in those cases,

they had the legal rights to demand that [inaudible] legal obligation to give it, so under the GDPR, I felt confident that in that case, such a request can be granted.

Now, that was before any automated access system. That was individual review, and I think such request would still best be handled that way, not in the automated system. So I'm perfectly comfortable with striking A as suggested by Brian.

UNIDENTIFIED MALE: So what you just said suggests to me that we should not strike A, we should keep the existing language, "Unless otherwise required or permitted, you don't do this."

JANIS KARKLINS: Okay. Ben, please.

BEN BUTLER: Thanks. Just wanted to point out in response to Margie's intervention, correlation in these types of investigations is important, but being able to search based on specific fields with the expectation of getting back all the other domain names that match that value, that's not something that we are saying has previously existed legally, and we're not saying should exist legally now. So just clarifying that. As far as striking A, I'm fine with that, and leave it to the manual process.

JANIS KARKLINS: Thank you, Ben. Chris, please.

CHRIS LEWIS-EVANS: Thank you. I think Volker's made one of the points I was going to make. The other side is if we do keep it, I would quite like to put another footnote on to the bulk access to reference the implementation guidance that was in the [inaudible] recommendations, because I think that's a good description of what we mean by bulk access and what we don't mean by bulk access. We've had a lot of descriptions and discussions around what we mean by bulk access, and what we don't want to do is limit multiple requests for the same purpose because that's [inaudible].

JANIS KARKLINS: Thank you. Margie.

MARGIE MILAM: The only thing I wanted to point out is that I believe European [inaudible] does reverse lookups as well, so I'm not sure it's illegal. I think that's something we should ask for legal guidance on. So I just wanted to flag that. I think it's .it if I'm not mistaken. They made a presentation in Morocco, so this is something that is not outside of – I assume they must have done some legal analysis on this and we could certainly confirm it, but that's my understanding.

JANIS KARKLINS: Thank you. James, please.

JAMES BLADEL: I was jus curious because it seems like if we're going to – and I'm treating these two separately like there's a bulk access where we're requesting presumably I'm sending a list of domain names that I would like a response on, and if I'm doing a reverse lookup, I'm sending one and then I'm following the breadcrumbs, so I get a contact response and then I go, "Well, what else does that person have or individual or entity?" And then I want to do a query on that domain name and so on. Maybe that resulting list then feeds a bulk access lookup.

I'm curious as to where the balancing test occurs in both of those transactions, if there's individual [pair-wise] balancing tests going out for each domain name that is submitted as part of a bulk access, and it fails, just that one would fail, right? presuming if you submitted 20 and two of them failed, the other 18 would go through.

And then I think that the reverse thing, it would be like at what point in that chain would that – if you had a failure at the second hop in a reverse lookup, would that then just fail the rest of the chain?

So I'm just trying to think of how this goes through, because Allan I think walked us through his test here earlier and I'm trying to figure out how you would cram a list of domain names down through that process, or if you even could.

ALLAN WOODS: [inaudible].

JAMES BLADEL: I don’t mean to put you on the spot. I'm sorry, that wasn’t my intention. I was just kind of throwing that out there for consideration, because if we have to do a test for each one of these, this complicates that.

JANIS KARKLINS: You're asking for the floor.

ALLAN WOODS: Yeah. My original point – I’ve put my card down, but I'll say to James that to be honest, if somebody asked me for a reverse lookup, so this is a domain which we believe is infringing our trademark, I'm just going to go there, and we want all other domains by that person, to me, I would only give the response to the domain requested, because there is absolutely no reason to give them all the other domain names because there's no indication that there is an infringement of a trademark in any of those domains. Even if incidentally there was, again, you're not asking a specifically made request for this and that would not pass the balancing test in my mind.

JAMES BLADEL: Can I ask a follow-up to that, Allan? Because if I ask you hypothetically to give me the contact information of the entity for this domain name because I believe it’s infringing on my trademark – by the way, Mark SV would like to be in the queue after me. Wow, I actually couldn’t think with that rodeo over there. Okay, so I like it though. I have to do it too. The curse of being at the end of the table and having one elbow free.

So going back to the question, if I ask you, I have a domain name here and I believe the domain name is infringing my trademark, it said James Bladel in it and we all know that that's a unique name, give me the entity, and then you gave me the entity, what is the assertion that I make when I submit the name of a person? I believe this person or entity is a serial trademark offender? Even though I don't know what the domain name is, I want you to tell me what the name is so that I can tell you if they're ... Does that make sense?

If you've got jamesbladel.com and I know that I'm jamesbladel.com, I can tell you that I think that's infringing. But if then you come back and say that the answer is Matt Serlin, how do I pivot with that bit of information and make a subsequent claim? I don't think we have to answer these here, I think these are questions that when we follow these things through, the balancing test starts to break down in my opinion.

JANIS KARKLINS: Okay. There were a number of reactions I think on the same topic. Mark, please go ahead.

MARK SVANCAREK: We actually did submit a use case for this, BC too. It wasn't just related to trademarks though, it was related to investigations of malware command and control nodes. So in this particular case, we would have determined that a certain domain name was being used in a malicious way and then come to some sort of conclusion that there were other domain names that are being used as a larger command and control

infrastructure, and there's not a lot of detail in the use case because I thought we would actually discuss it, but we had to prioritize them.

Then at that point, we would come to the contracted party with a bucket of evidence and say “This is the investigation that we have done. Here's how you perform your balancing test in order to make yourself comfortable with the fact that we are now asking you to do a reverse lookup.”

So we never actually went through the details of how you would conduct such a thing, but it was really based on the idea that a bunch of investigation had already been done and so you could have a proposition and say here's why we think you should perform this test, please do it. It’s still subject to the data controller to decide whether to do it or not.

ALLAN WOODS: And I'm purely being devil’s advocate here and I don't even know if I believe this or not, but I'm just going to say it, that just because one domain is being used in such a manner does not mean that all other domains are going to be used in that manner that are owned by that person, and just to cap that off with – I think I said this in the chat earlier, that even criminals have rights. But again, devil’s advocate.

MARK SVANCAREK: Yeah. Like I said, we never had a chance to really discuss it. I do think it’s going to be a case that will be tested at some point, because there are reasons to have that discussion, I think.

JANIS KARKLINS: Okay. I think Brian is now in the line.

BRIAN KING: Thank you, Janis. Building on this conversation, I think we can find some comfort and maybe James can find some comfort, I think we don't need to worry about what the outcome of the balancing test might be to do this building block. I think here, if we're talking about the query policy and what you can query, we know you can query a domain name and [pull] back the associated data.

I think what A says is that if you're required to do the queries based on wildcards [inaudible] the registrant name, like the registry agreement requires if you choose to offer that, then that's something that could happen. I think in those cases, the balancing test might be a little different. It might come out differently than it would if you were just querying a domain name, and the person who owns the domain name, depending on what's alleged and the other things that go into the request might impact the outcome of the balancing test. But I think for this building block, we might not care that much because we're just focused on what goes into the query itself. Does that help us?

JANIS KARKLINS: Can't we think in the terms that as a default position, all these things like bulk access, wildcard requests, reverse lookups, Boolean search capabilities would not be allowed? That would be kind of the general premise, unless – and then if there are specific demonstrated evidence

that something may happen, like you said, Mark, that you would come to the registrar with the evidence that you think that this chap is a serial wrongdoer, so then that would be acceptable as a policy guidance – as an action.

So maybe something along those lines we could think of, general no, but if you can prove that there is a reasonable evidence, then we can accept that. Something like that. Stephanie?

STEPHANIE PERRIN: Yeah. I think again here, this is something where a template may help us work our way through this, because private sector, even Msoft, they can't just come in and say we think this guy's a crook, even if they're doing the same investigation as the police force might be doing.

So either they do like the administrative law parts of governments do where they bring in a police – a criminal investigator [just fine for] their access requests, we may have to do that in some of these cybercrime-type investigations to make it work under data protection law, or they don't have the protection that law enforcement has for some of their requests. Am I right here? In other words, they're going to have to prove to an Allan why they think this guy is a crook. Even then, it might not be enough, it might not meet the standard to have this kind of search capability or [release] capability.

An easier way to do that is to work through law enforcement. I know that you haven't been doing that, but that doesn't mean you don't [have to start.]

MARK SVANCAREK: Sometimes we do. There are all kinds of flavors. We work with law enforcement. Sometimes we post bond. There's all kinds of permutations of this thing.

STEPHANIE PERRIN: But it's a problem that has to be fixed in some other way than accrediting you as a cybercrime investigator at Msoft, [if you see what I mean.]

MARK SVANCAREK: Oh, yeah. That was orthogonal to this use case, it was we have to make a case, the actual details of how the case is made, were never really went into. Could have been discussed but were not discussed. And at the end of the day, it was still subject to the data controller making their decision on whether or not the case had lawfully been made.

STEPHANIE PERRIN: And because they have to defend that in court on legal grounds basis, they may just have to refuse it even if they suspect you're right, until you come in with something. Yeah.

JANIS KARKLINS: So Brian, then Hadia, and then Marc.

BRIAN KING: Thanks, Janis. Stephanie, to your question, I think for the purposes of this building block, we might be able to say, "Yeah, that guy is ab data accuracy guy and I want to request whatever domain names he has." That'd be a tough 6.1(f) to overcome, but I think what we're saying here is that the SSAD won't block you from putting the request in. Someone's still going to have to evaluate it, and there's a good chance that if somebody's doing real bad stuff and they have one other domain name, and it's related to the thing – none of which we know, because we're just asking for data – then 6.1(f) could come out.

I think what we're trying to agree here is that let's not say that we can't ask for the data, and this is just about the query policy. So the 6.1(f), the balancing and all that stuff is another building block. So I think we could do that here. Thank you.

JANIS KARKLINS: Hadia, please.

HADIA ELMINIAWI: I guess whether we leave A or remove it, we must make sure that the system is capable actually of performing this, and then putting it off or on is another thing, but we must ensure that the unified access model is actually capable of handling that feature.

JANIS KARKLINS: Thank you. Marc Anderson.

MARC ANDERSON: Thanks, Janis. When we started this conversation, I thought it would be pretty adamant against any of these things, and then listening to Volker give an example of when he provided bulk access to law enforcement and Mark SV's botnet use case, compelling stories, but I also though listening to those, I don't think either of those are good use cases for an SSAD system. Those are very specific, very individual requests, and I think those are much better suited for one offs under recommendation 18 from our phase one report.

We've always talked about how recommendation 18 doesn't go away with creation of the SSAD. There's always going to be need to address some number of requests that don't fall into this SSAD system, and I'm not sure that building an SSAD system taking into account these very corner cases like this ... Botnets don't come around every day.

You know what I mean. That's not your most common use case of a lookup. So this has been an interesting conversation. It did not go the way I expected it to, but I think my intervention here is to point out, let's not try and build the SSAD system to account for every single corner case. I think we need to narrow this or tailor this for the most common types of requests we're going to be dealing with, and let's try and avoid going down some of these ratholes for corner cases, niche cases, especially where it's going to be very highly subjective as to whether you release the data, such as Volker's example earlier.

JANIS KARKLINS: That's why I suggested that maybe we can think as a default position that that would not be acceptable but then there might be exceptions

and then this needs to be kind of proven, and then that would be considered. Not allowed, but considered.

Margie I think is in line already for a while. Margie, please.

MARGIE MILAM: I think it's not as edge as you think, Marc. In another example is fighting phishing attacks. Phishing attacks, at least where I work, are daily or regular occurrences. And to be able to do a search on the contact field, the e-mail address for someone who's doing a phishing attack is something that's not an edge case and would benefit from the efficiencies and scale and operations that would come from the SSAD.

So I would encourage us to allow those kinds of use cases, not prohibit them but perhaps be selective in them and recognize that it's perhaps not such an easy balancing test issue and it may take a different approach to all the other requests.

And the other thing I wanted to point out is I guess I'm probably less interested in Boolean searches and wildcard – I think really what I'm focusing the most on is reverse lookup of an exact contact field. The other part of it is less necessary, at least from when I look at the use cases that are most important. Thank you.

JANIS KARKLINS: Thank you. Allan W, Alan G, and then Matt.

ALLAN WOODS: Thank you. Two very quick points. One – and Brian, I agree, we're talking about creating policy here, but I just wanted to kind of preface and say that one of the hardest and most occurring abuse tickets that I have to answer is when a person comes to me and says "This person is breaking the law and I want you to stop it." And I'm like, "I can't, because I am not the police. Go to the police."

So down the line, if we are leaving that kind of a query in, we must ensure that we put a pin on the mark saying if a registry or registrar turns around and said "I can't make this call because I'm not the police," it needs to be accepted as well and needs to be, yes, fair enough. So that's important.

And just on Margie's point, again, we're very sympathetic and everybody should be very sympathetic to the fact that it would be exceptionally useful to have this data, but we need to guide ourselves again by what is legal, not necessarily what is useful and would be amazing for us to have.

I agree we'll find a way. This is the whole point, making it simple, but what is legal as oppose to what is useful must be our guiding light in that.

JANIS KARKLINS: Thank you. Alan G.

ALAN GREENBERG: Thank you. I guess my caution is to not delete something from a request possibility. Two reasons. Number one, you don't really want to have to

tell people about multiple ways of submitting things and give them the fine distinction between which to use for what. This may not be processed automatically, but having the same entry chute into the system is really beneficial. So you don't have to explain things, you know what gets in queue, it's logged, all sorts of things happen when it goes through this path, which might not happen if it's going to be submitted to one of 100 different registrars. So there's all sorts of benefits from using the same entry path.

The second one is this is going to evolve. The law will change eventually, our methodologies will change, and our understanding of what we can and should do will change, and this says we're not changing what is presented to the user. It all goes in, some will be handled manually, some will not be, but they're all handled in a uniform way.

So there still may be edge cases which just don't fit the form, and so be it, but I think to the extent possible, we should [inaudible] a single entry.

JANIS KARKLINS: Thank you. Matt, please.

MATT SERLIN: Thanks. Just a couple points. Margie, you're right. the usefulness for reverse WHOIS for phishing instances obviously. But a couple of things. So number one, that really only works in a centralized system. You're used to running reverse WHOIS lookups in the old WHOIS paradigm where third parties aggregated all of the WHOIS records.

So if we develop a centralized system, then a reverse WHOIS lookup is extremely useful. If we have a decentralized model, its usefulness is dramatically reduced.

The other point that I wanted to bring into the conversation that actually was happening in the chat – I don't know if everyone saw – is that we're talking about some of the good potential uses for things like phishing and fraud and things like that, but Farzaneh and James had a very good point. Think about the flipside of that, so a government that wants to identify all of the domain names that a political dissident has registered can use this reverse WHOIS lookup utility for that as well.

So let's make sure that when we're thinking about these, we're also thinking about some of the unintended consequences that these policy choices could have. Thanks.

JANIS KARKLINS: Thank you. Mark SV:

MARK SVANCAREK: I wanted to confirm what Matt said about the efficacy of the thing. There are a whole bunch of really powerful techniques that are not going to be available going forward, so even with this reverse lookup there are a whole bunch of heuristics that you could apply like pattern matching and things like that, not exact matches. That stuff is just gone.

And as you say, in this case, if you're doing a reverse lookup across a very small set so a small registrar, not very helpful. A thick registry,

more helpful. But again, you're looking across a much smaller pool than you ever were before, so yeah, the whole thing is ...

So if you're talking about utility of it, diminished. If you're talking about the risk of it, also diminished.

JANIS KARKLINS: Alex, please.

ALEX DEACON: Yeah, I think Mark said what I wanted to say, but again, just to Matt's point, I think it would be possible – it is possible, I believe – to do a reverse search in a distributed system. Technically, it's absolutely doable. Would it take some time? Yes. Would it be cumbersome? Yes, but it would absolutely be doable for sure.

JANIS KARKLINS: Thank you. Allan.

ALLAN WOODS: This is a slight aside on what you just said there, and it kind of hits me in the heart slightly where you're saying that there's a lot of really good tools out there and heuristics that are no longer available.

To me, that's not something that needs to be brought here. I think that's something that the security industry needs to bring to people like the European Commission and say, "Hey, you broke a lot of stuff here." All we're doing here is applying the law, and we are so sorry that we're

breaking stuff in order to do this, because let's be honest, we all have a benefit from what you're doing and what Microsoft and other security people are doing.

But we can't fix the ills of this because we have to deal with what we're doing. I can only say, please, bring it to other places as well.

MARK SVANCAREK: Yeah. I'm sorry if I was implying that. Yeah. I was just trying to acknowledge that what we're – anyway, you get it. Sorry.

JANIS KARKLINS: Yeah, one thing we got all, that life will not be the same as before GDPR, so that is for sure and that probably is the main conclusion that we need to always remember.

I think we're slightly tired. At least I'm gradually shutting down, and I would like to maybe suggest that we stop here for today, and thinking about tomorrow, I remember that Marika told me I need to ask you to read legal memos still tonight, especially when we finish 15 minutes early. So you have 15 minutes still to work.

But honestly, I don't remember why we need to do that, Marika.

MARIKA KONINGS: Thanks. I think it's especially from our perspective very useful to get input from the group which concept or which aspects will guide the subsequent drafting of the zero draft.

I thought the conversation this morning was really interesting and very helpful, and I'm kind of worried if we take that conversation to future calls, it may not be as productive, so I was just hoping, that was my suggestion to kind of see if people have time to read through them and kind of come back with what you think are the most relevant points that need to be factored in as we move to kind of the next draft. That will give us some guidance, may also kind of flesh out what aspects may need to be further discussed or considered. And again, hopefully make our calls after this meeting more productive and more focused.

JANIS KARKLINS: Yeah, but you're talking about concepts from legal memos that we – so look, tonight, you will not have that much wine as yesterday, because you will need to pay for wine yourself, which means you will be soberer and you'll be able to read memos also tonight, not only tomorrow morning.

Jokes aside, so please, try to read memos that we could talk about them tomorrow and see what kind of assessment form the first reading of memos we can bring and factor in – staff can factor in working further on the draft. So that would be the first part of discussion.

The second one, we still have a few building blocks, including this one, on query policy which is on building block I that we didn't touch today. We talked about building block L on query policy. But there are a few other building blocks that in my view need to be revisited even for a brief time.

So we would go through those and I will try to provide maybe list sequence how we could do it, and we would finalize, time permitting, the policy principles just to see whether there is any hard feeling about policy principles and also with understanding that they may evolve as we progress in our conversation on building blocks.

And then the last one, we will tomorrow talk in early afternoon, maybe at 1:00, how to sketch out our work to Montreal and beyond. So I will try to outline my thinking to see whether you would accept that or not. So that would be my proposal for tomorrow, and I see that Alan is wishing to say something. No.

So with absence of a request for the floor, I consider that we're done today. Thank you very much everyone for active participation. I have a feeling that we progressed at least on a number of issues reasonably well. Staff got some ideas what will be reflected further in the 1.0 draft.

And with this, I wish you all a very good return to hotel, and good evening.

ALAN GREENBERG: We start tomorrow at 8:00, I believe. Correct?

JANIS KARKLINS: We start –

UNIDENTIFIED MALE: Who are we applauding right now?

JANIS KARKLINS: No, we start at –

[END OF TRANSCRIPTION]