ICANN Transcription

GNSO Temp Spec gTLD RD EPDP – Phase 2 LA F2F Day 3

Wednesday 11, September 2019 at 1530 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 the agenda wiki page:
https://community.icann.org/x/6oECBw

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

JANIS KARKLINS: Good morning. Thank you for coming back for the last day session. Today we have planned to go through legal memos because staff suggested this is still important, even to gather initial reflections on them. I hope that you had a chance to read them. Once again, it's a long reading. It's about 40 pages. Then we will probably wrap up with Trang. I will try to summarize where I think we are, and we'll see [by] our body language whether you're in agreement with me or not really. Then we will maybe discuss a little bit a proposed way forward with work for the next few months until the initial report is published. So that's the plan.

Before we go to legal memos, maybe we can sum up where we ended yesterday on query policy. My understanding is, when it comes to issue that we discussed yesterday – [the link] on the reverse lookup and bulks requests that I understood the majority

could live with a situation or formulation which would suggest that, in principle, the existing practices in this respect would be discontinued; in other words, as a general principle, no bulks requests, no reverse lookups, no [Boolean]. That's a new term for me just recently. Still not sure that I know what it is, but nevertheless, sounds good to me. But in a case which is clearly justified and proven by evidence, these practices could be used on exceptional bases. So that is where I think we could land in order to accommodate views expressed yesterday at the table.

James?

JAMES BLADEL: Thanks, Janis. Good morning. Thanks for summing up where we left on this because I left here yesterday feeling just a little uneasy and unsure of where we were going with reverse search and bulk access and Boolean operations on the data.

After talking to some folks and drinking some strong beers and thinking about this last night, I want to say first off that I have no question or doubt on the usefulness of these facilities in investigating cybercrime or trademark infringement or anything like that. But I think we need to take a hard look at what we're actually talking about when we talk about these things because I feel like, with some things we're dealing with, we're just coping with side effects and unintended consequences of privacy law, the GDPR and CCPA.

But some things are right in the bullseye of what these laws were seeking to address, which is the privacy rights of data subjects. I

say that not to shelter the percentage of folks, the very slim portion of folks, who are actually doing bad things, but we have to also think about the 99.99% of people who have done nothing wrong and who are entrusting providers, registries, and registrars to protect their data. Regardless of what our obligations under the way are, we have a relationship with these folks who have opened their wallets and have shared their personal information with us. They may have something in their account that is unrelated to something else in their account. If there's a political or religious or a lifestyle type of thing that can be gleaned by that, I think we have to be very, very careful.

So I just want to put out there that I think we need to examine this a little bit more closely. We already provide this service under legal due process with warrants and search warrants and court orders and that thing, but putting into a SSAD system is something that I think a lot of registrars, including GoDaddy, would probably resist. Even so, I also think that, if a registry offered that, we would probably be reluctant to share our data with them as well, just because I think that would violate the trust that our customers have put into us.

So I think we need to think about this a little bit longer and a little bit harder before we just say, "Yeah, it's okay. It's optional. You can have it if you want it." I have some concerns with that.

JANIS KARKLINS: No, I'm not saying that it's optional and you can if you want. I think what I was trying to say was that there might be situations where that may be extremely useful for investigation purposes and that

each case should be proven. It's not just somebody says, "I want it this time. I don't want it tomorrow. I want it today." No. But if that can be proven by evidence, by [inaudible], we can develop some kind of criteria of what that would mean. So then, on an exceptional basis, that would be allowed in practice.

JAMES BLADEL: I feel like we have that today, and the exceptional basis is, for law enforcement, we require a search warrant. For private parties, we require some sort of a court order or a subpoena, and we have courts and legal functions to provide that. I don't think we need to recreate that within the scope of the ICANN policy. Those exceptions to me are very important, but they're already addressed by existing legal facilities. That's just …

MARIKA KONINGS: I just want to ask the question. So the language as is, you don't see prohibiting from what you're already doing today.

JAMES BLADEL: Yeah. I mean, think we just need to spend a little bit more time on it. My initial reaction is with the first clause of, "Unless required or permitted." If we strike that, then it just said that this is a blanket prohibition of this system. This is an extra legal system that we're building outside of the legal and due process framework that everyone enjoys from whatever country they live in.

It doesn't belong here, in my opinion. Thanks.

JANIS KARKLINS: We have a few requests. Again, we will try to propose language, but I need to reconfirm whether my sense was correct.

Brian, please?

BRIAN KING: Thanks, Janis. James makes a lot of good points there. I think I could maybe propose something that might meet in the middle, so to speak. A thought that I was kicking around for this is I certainly understand the concern that this could be used to identify entire registrants' domain portfolio, which might contain other sensitive domains. I don't see this kind of thing – I don't want to preclude it, but seems to me this would be a 61F. It might be [manual] scenario.

So what if this type of thing was only allowed within the SSAD after someone had already done a query on a domain name and then it was a pivot from that? So by just being used where a domain name is alleged to be infringing and the requester is promised to do everything that they need to promise to do and allege that this is an infringing domain name and then to pivot and say, "What else does this person who I'm pretty sure are infringing on my rights or committing a crime or doing something else bad have?" Would that give any comfort to the contracted parties?

JANIS KARKLINS: Yeah, please, James.

JAMES BLADEL: Just to respond, Brian – I appreciate your efforts to navigate between some of the different difficult rocks that we're sailing around – I just want to, I think, reiterate that, in that scenario, I feel like we need to elevate this out of SSAD, out of ICANN, and into the legal arena, where not only do we have courts to review that and see if it's warranted or not so we don't have to make that call as a private party, but also you have lots of other leverage you can pull in terms of warrants and subpoenas and court orders that get you a whole bunch of other data, not just registrant data but payment data, IP data, and session data. If it's that bad, then it warrants, I think … Because, if it doesn't, if it isn't that bad, and we do build this in, then I would suggest that we have violated the privacy of the folks in this system who have done nothing to warrant that kind of a thing. If it's that bad, I think it needs to come out of this system and go into the legal arena because I think we have – I don't want to drop U.S. stuff, and I'm not a lawyer here – constitutional protections against people coming into your house in the middle of the night and looking in your garage and saying, "What else do you got in here? Can I see what you got under your mattress? It might be useful to me?" "Sure, it might be useful to you. I'm not doubting that it might be useful to you. But it's my house. Get out. If you want, come back with a warrant. Now you can do whatever you want." I feel like we're trying to say, "Let's build this loophole in what people enjoy as RIPE today and build this system that has this loophole, this trapdoor."

I don't know. I just feel like we need to spend a little bit more time on it. We need to get some legal advice. But just commercially, I

don't know that I could look in my eye and tell them that I agreed to this and that this is okay. If they're a bad guy, I'll throw them overboard in a heartbeat. Do what you want with them. But most of them aren't bad guys.

Anyway, I don't mean to editorialize here, and I certainly don't mean to blow up our agenda. I see there's a big queue, so I'll just zip it.

JAMES BLADEL: No, no. Again, we are here looking for the consensus, and I'm trying to reconcile what I hear, different positions, in a way that would allow everyone to say, "Okay, I can live with that." That's my goal. If I can achieve that, I'm happy. If I cannot achieve that, then we need to spend more time, which we will be certainly doing now, since many flags are up.

Ashley, your flag was up and you put it down.

Okay. Then Margie was next.

MARGIE MILAM: Thanks for sharing your concerns, James. I think you're right in the sense that it needs more thought. I think maybe not today but another day we should really delve into it because we're not proposing the same kind of reserve lookups that happened before GDPR. There needs to be limits to it. There needs to be evidence like Janis was saying so that customers that are truly not involved in really bad acts are not affected by it. There also could be additional safeguards, additional bonding – whatever – so that the

person that's actually making the request is living up to a higher standard. So I feel like we actually need to do that.

We also need to evaluate the legal analysis because, if the answer is not possible, then that ends the discussion. I know Alan was pointing that out yesterday. So I just want to flag that I do think that it's important to do it and to do it very narrowly.

But I do think that, because the policy that we have doesn't, for example, take into account the difference between a legal and natural person, there might be areas where we actually could do reverse searching and have less risk. For example, if the reverse searching is on the org field and the org field is a legal entity, the risk of having a privacy concern has gone way down, if that's one of the things that we could explore. So I'm just merely confirming that I think it needs more analysis so that we can get to a place where it's not viewed as a repeat of what happened before GDPR.

JANIS KARKLINS: I have only one warning. We do not have too much time. Saying on every issue, "Let's keep discussing it and any time after," then we're simply kicking the can down the road and we need to find a way how to get to the compromised results as soon as it is feasible. I'm not rushing, but I'm just saying.

Maybe in this particular case it would make sense to establish a four-people small group and see where the divergent interests on the top or the divergent views on the topic are and then see whether that small group could work out something that could be then presented to the team. Again, I'm not saying that we could

constitute that small group to work now, here, but let's say to do it within that small group outside the plenaries within the next ten days and then come back with the textual proposal for the consideration of the rest of the team during one of the calls.

I think that is Thomas who is next, followed by Milton.

THOMAS RICKERT: Thanks very much, Janis. Good morning, everybody. You might remember, when I introduced the first use case, I put in safeguards. Two of them were no Boolean search and no reverse lookup. Some liked that. Some have called me and criticized me passionately for putting those words. I have to confess I didn't put that in there. I think I explained it at the time and I will explain it again because I'm taking sides for one or the other because I think we need to be respectful of what we're chartered with. We're chartered with reviewing the compliance of ICANN's dealings with registration data. So we're looking at ICANN's existing processes and making that system compliant with the privacy laws, particularly with GDPR.

Before the EPDP was started, ICANN did not offer Boolean search. They did not offer reverse lookups. You found that with commercial vendors, but that was not an ICANN service previously offered. Therefore, I think that it is not within our charter. So I think we can't even work on that because it's not in the scope of the things that we have to review.

So I'm not trying to shut off this discussion, and I certainly appreciate that many in this group find this very useful. But I think

that that would be a separate PDP, whether ICANN wants to establish that. I think this is just not the place to be discussing this.

JANIS KARKLINS: Thank you, Thomas. Milton?

MILTON MUELLER: I really just wanted to mainly strongly agree with James was saying. I think the key problem we're having here is that we are forgetting what we're actually supposed to do, which is what Thomas just reminded us of. There are all kinds of reasons why you might want to get all of this more elaborate data, but that's not what we're doing with the WHOIS system. In fact, it was these kinds of activities and practices and indiscriminate forms of searching that led to the legal problem to begin with. So all we're doing now is trying to make ordinary WHOIS confirm to GDPR and have a process for disclosure that is consistent with the legal basis.

As James pointed out – I don't see how you answer this question, and it's depressing to me that we're still debating this – there are subpoenas, there are other law enforcement mechanisms, by which you can get this and more: credit card numbers, accounts, everything you want if you have a proper search warrant. The purpose of WHOIS is not to give you that, and we shouldn't be redefining its purpose in this way. Again, it's flabbergasting to me that we're having such a basic discussion this late in the game.

JANIS KARKLINS: Thank you for acknowledging lateness in the game. That's encouraging. Alan G?

ALAN GREENBERG: Thank you very much. I made a plea yesterday that we should keep the request queue open, regardless of whether we're responding or not. That allows us to essentially future-proof this and accommodate things that change.

I'll point out that – there can be whatever caveats, saying there's not a chance in hell this is going to get answered unless you have a legal order but still accommodated because that may change – we have IETF development work/standards work going on with reverse search within RDAP. So the capability could well be there without intervention.

We have a legal/natural discussion that we still have in this phase, and we also have organization field, which in some cases will be putting in and saying "Publish." So we may well have a basis for doing limited reserve searches that don't violate individual privacy, perhaps in an automated way in some cases. The world is changing around us, and I think the request should allow it with whatever caveats we want about the current data because that could change going forward. Thank you.

JANIS KARKLINS: Thank you. Stephanie, please?

STEPHANIE PERRIN: Thanks. So many things to say on this, but I think I'll just offer the Civil Society perspective because I agree with what Milton and James said. From a Civil Society perspective, the enablement of private sector surveillance is one of the biggest threats to privacy on the horizon. Yes, this has gone on. The outsourcing of this kind of searching to the likes of domain tools who are what [TREM] refers to as low-hanging fruit in the lawsuit category gone on for years. It doesn't mean it was legal. It doesn't mean it was acceptable. It was however legal for law enforcement agencies and other organizations to hire those services because they didn't keep the data within there in the no [MB] decision dating back to the ['90s]. It's been downhill ever since, [Joy's point] being one of the more controversial instances.

So all I'm trying to say is there's a big history here. We are looking for more case law at the Supreme Court level to substantiate that charter protections and constitutional protections also apply in private sector instances, particularly when the public sector is relying on them. That is what this means to us. I hope everybody follows that.

But go for this. Build it in because maybe we should just in case we can get away with it in the future. I'm being a little unkind to my colleague Alan's characterization of this. It's [inaudible]. It's a red flag in front of [bull]. Thank you.

JANIS KARKLINS: Thank you. Mark Sv?

MARK SVANCAREK: I lifted my card for one reason. I'll get to that one last. Just responding to previous interventions, I think I've heard a couple mentions of things like credit cards and stuff like that. We decided that that would be out of our scope the last time we were in L.A. So it's interesting but I don't think it's applicable to this conversation. We are not talking about that, and we decided that we would never be talking about that.

We decided yesterday that we were talking about the future and not the past, so, while it is true that there were services like domain tools in the past, we're not talking about those capabilities anymore. We clarified this yesterday. We clarified yesterday that we were talking about searches within a single entity, whether that's a registry or a registrar. We were not talking about a complete aggregated data set. So, if it wasn't clear yesterday, please allow me to clarify that today.

I do think that the issue about legal/natural and org fields is pertinent to this. So just putting that out there.

But the real reason I lifted my card is the transport issue. I think I mentioned this at a previous meeting. I think it was Marrakech. Maybe it was Kobe. When we talk about that the SSAD will do X, I think we need to clarify what do we mean by that the SSAD will do X and distinguish that from what RDAP can and will do. So RDAP is just a transport protocol. It's the way that I make a request, and it's the way that data is delivered back to me.

The capabilities – it's too bad I had too much other stuff because I actually had this formulated. I've always made the point that, when we say there's no bulk lookups, that's not to say that RDAP can't

be created a certain way or that multiple RDAP requests can't be made that are tantamount to – somebody could argue that until bulk lookup is defined. So I just want to make sure that, when we say this doesn't work in SSAD, it doesn't mean that it doesn't work in RDAP.

The distinction that I'm making is that, if we're having an extraordinary request, one of the ones that we talked about before but not yet defined, there's some safeguards involved. A preliminary investigation is made. Somebody is making an extraordinary request. I wouldn't want to rule out the fact that the idea that the fact that that extraordinary request could be delivered by RDAP or that the response could be delivered by RDAP. I want to make that distinction. So that's just: there's a system that's being created by contracted parties based on RDAP. They way that it responds to requests is defined in various profiles. Should there be a profile created that allows such an extraordinary request to be made and responded to, I wouldn't want this policy to prevent that.

So, if extraordinary requests are going to be through e-mail, that's great. We already great that that's not part of SSAD. If we decided that, by policy, SSAD does not support these types of requests … I hope I'm making my point clear. I feel like I'm talking in circles. Am I? Gina is shaking her head. So maybe I'm not clear.

UNIDENTIFIED SPEAKERS: [inaudible]

MARK SVANCAREK: Okay. Here's an example. There was a suggestion in earlier discussion that SSAD cannot be used to collect public data. If SSAD is a concept, then you could say SSAD cannot be used to ask for public data. But we know that RDAP is being used to request public data. So, conceptually, what's the boundary between SSAD and RDAP? So these are questions I've been asking. They're technically pedantic. I just don't want to paint ourselves into a corner at a policy level by saying the technical capabilities that are built by someone are … yeah. What we can't do in policy … The things that policy prevents us from doing in "SSAD" don't prevent us from doing things outside of SSAD, which may use the same transport. That's what I'm trying to say. I don't know if I'm getting my point across. Like I said, it's a pedantic issue. But I think it's important for implementation. Thank you.

JANIS KARKLINS: Two elements in that. We are working on the system of WHOIS lookup being compliant with GDPR. But GDPR equally applies to every other activity. As a result, whatever other systems you are referring to ultimately should be compliant with GDPR as well. That's the point.

MARK SVACAREK: Well, we discussed this yesterday at some length, that the extraordinary request also has to be a lawful request and it's subject to a balancing test. What I'm saying is that the way that you deliver the request to a contracted party could be using the same transport that you use to make normal requests. I just

wanted to be clear that we are not boxing out the use of that transport to make different types of lawful requests that are not envisaged under the SSAD policy.

JANIS KARKLINS: My question is you heard James saying that, if you have a court warrant, you can check everything in his garage. So what you call extraordinary situations – would it be conceivable that, prior to putting the question in for the bulk search, you would go to the court and say, "We have suspicions that this guy is a serial wrongdoer. Please give us a warrant to look up wherever else he could have planted his (whatever)"? Is that something feasible, or do you not have a right for doing that?

MARK SVANCAREK: No, I think that's what we agreed we would do in those cases. For example, I've done an investigation. I've determined that a reverse lookup is justified. At least I'm asserting that it's justified and I have certain ways of backing that up, whether I'm working with law enforcement or however we believe that this is a lawful request. Then we make this request somehow. Maybe we call someone on the phone or we send an e-mail or maybe we make a request through RDAP because RDAP might have an extend protocol that allows me to request such a request and append the data or whatever. This is completely theoretical.

Then, once the request has been made, once the balance test has been performed, if the request is judged to be lawful and the data is now going to be returned, it would be great if the data were

returned by RDAP in one of the defined protocols because that allows me to put it into my same system where it can be consumed in my same system whereas, if send me a bunch of data in an e-mail, now it has to be processed differently and put into the system where it could be modified or corrupted or whatever.

So it would be very nice – I don't think it impacts the lawful of the thing at all – if I could use RDAP as a transport for delivering the data back to me. I don't want us to prevent that by a definition [of] policy. That's all I'm saying.

JANIS KARKLINS: Thank you. We have next Brian in line.

BRIAN KING: Thanks, Janis. I think I'm going to try to nudge us a little closer to something that we can agree on here. I think, to be clear, what we're getting at here, by proposing that we strike A, is that we're not trying to make this a system requirement of the SSAD, that these things are required. All we're trying to do by proposing the strike [of] A is to say let's not explicitly preclude those now. Alan mentioned there's work at the IETF that's going on that may make this a more formal thing and may enable this in the future. I'm sympathetic to some of the points that were made, that if this kind of stuff isn't in the scope of the EPDP, without saying whether I agree or disagree with that, to talk about wildcard requests and these kinds of things – and it's probably not in scope to preclude

those things either in a future stage … Again, striking A would fix that.

Most importantly for us, the Boolean search capabilities and the wildcard requests are things that are in the base registry agreement now. So, by not precluding – it's like a double negative – those from being in the SSAD – leaving the door open to future policy might enable that – that will allow registries to have all of their stuff come in through SSAD, rather than have to support, as the RA requires now, them to do it on their own. The way this is written would preclude SSAD from doing that, I guess. So striking that would adjust that, too.

Again, we're not saying to make this a requirement of SSAD, but there seems to be a lot of consternation about it. So, if strike the preclusion, that might fix this. Thanks.

JANIS KARKLINS: Thank you. Chris?

CHRIS LEWIS-EVANS: Thank you. I'm not going to go over what I think about reverse lookups. I think everyone knows how useful it is for us and the GAC's views on that and our advice on it.

What I really want to touch on is Boolean search capabilities on this. [inaudible] should be used to minimize the data going to data subjects. If you use an ["and,"] you're restricting data. So why would not want to do that? Just a question. Thank you.

JANIS KARKLINS: Thank you. Alan and then Volker.

ALAN WOODS: Thank you. I suppose I've just two very brief points. One is I would like to call everybody's attention to what Thomas has said. I think we didn't possibly put enough thought to what he had said because what he said actually has a lot of weight in it. That is we really need to limit ourselves to the charter here. He made some very good points. I think it should deserve a little bit of thought by the group as to where we're going because, at the moment, we are trundling down the rabbit hole. I think perhaps we shouldn't be. So I agree with Thomas on that one.

In response to both Alan and Mark, again, we get the idea that– and even Brian just said it there as well – we don't want to preclude this from the future. Apologies, I'm going back on my word and I'm just going to reference the GDPR as the highwater mark here, but we have to focus on Article 25 as well, which is privacy by design. We can't put into our very design saying, "Look, this is the limitation with the idea of the privacy rights of our registrants right here. However, in the future, we might add this ridiculously open backdoor as well, just in case we ever need it. We're not going to use it now, but we're going to design it in just in case that backdoor is available." That's exactly what you're saying.

At the moment, we are creating a new process. We're trying to create a new policy that leads to a process which is going to

respect the privacy rights of the registrant, not the usefulness of that data for third parties. That's what we need to focus on.

JANIS KARKLINS: Volker, please?

VOLKER GREIMANN: Maybe just one final word. We're here to design the SSAD, not anything that the RDAP protocol might also be used for. Let's stick to designing the SSAD and not try to design in other things that are not part of the SSAD but might be useful at a later time. Let's stick to the subject matter that we have. It's a complex enough issue. It's a big enough topic to keep us talking for ages. Let's hope that we manage to further [inaudible] earlier. Let's not stick in other discussions that may be useful for a later time just because they might fit in here as well. Let's design the SSAD now and not anything that we might be able to use or make available at a later time. Thank you.

JANIS KARKLINS: The last word from [the BC and] Mark, please.

MARK SVANCAREK: I'm worried that what I said was misrepresented or misunderstood. I'm not saying let us design future capabilities into SSAD. What I'm saying is that, when we get to implementation, let's not make sure that various implementations, which are lawful and outside of

the scope of SSAD, are not precluded. So this is not related to this policy.

I'm going to set this aside for now. I don't think I said really what Alan is worried that I said or that Volker is worried that I said. If it comes in specificity, I'll raise the issue. I was making a general statement. I think maybe it wasn't helpful. Maybe it just muddied the water. I've planted my flag. So, when I make these very specific objections, that's what I'll tie it back to.

So I apologize if I just added complexity to a conversation in a place where it didn't need to be added or if confused things. So, apologies. Thanks for listening. If it pops up again, now you'll know why I'm talking about it. Thanks.

JANIS KARKLINS: Thank you. Then my question to you, Mark and Margie, is whether you can accept that we, as a general principle, mention no reverse lookup/bulk requests for the purpose of policy we're working on. If you cannot accept that, you heard there's a lot of concerns around it. If you want to continue that conversation, then I would suggest that the BC and the registrars – one of you [from each] – get together and then try to work out language/an editorial proposal. If someone wants to join that couple, please feel free. And the Secretariat – yes?

UNIDENTIFIED MALE: [inaudible]

JANIS KARKLINS: No, I was talking about you.

Yes, Alan, please.

ALAN GREENBERG: Just to point out, as was noted yesterday, we're using the term "bulk access" in two distinctively way: one here and one [for] someone making 30 requests roughly at the same time for individual domain names. Let's make sure, when we use the words "bulk access," that we differentiate between them or come up with different definitions so we don't have confusion as to which we're one we're using in any [inaudible] case.

UNIDENTIFIED MALE: Agreed. We should call the other one "high-frequency access."

UNIDENTIFIED MALE: [Yeah].

THOMAS RICKERT: Janis, I apologize, but you suggested that we [inaudible] the sub-team to work further on this. I was hoping I would get a response to my point of order regarding the charter question. I think we can't take that on, even if we wanted to.

JANIS KARKLINS: Okay. When the two meet, please also factor in the point of view of Thomas. Again, we can now do another round and we will hear

exactly the same thing. So what we need to do no is see whether there is any way we can bridge this and if a bridge is even possible. If a group of two would come to conclusion that a bridge is impossible, then one would say, “Sorry. This time we lost. So we need to go further on this subject.”

Stephanie, please?

STEPHANIE PERRIN: I’m confused. Note that I don’t normally start with “I’m confused.” The point of order is that we cannot work on that. That includes the sub-team. Let’s do a vote on the question of the point of order because it’s outside the charter. The IETF wants to work on that. That’s their business. They’re not chartered by the GNSO to figure out the replacement for the rest of it. It’s outside our charter. Replacing domain tools is outside our charter.

JANIS KARKLINS: I hear you. What I’m asking is, since the zero draft – we’re talking about formulations of the zero draft – “Point A. Unless” … I will find it on my screen. “Point A. Unless otherwise requested or permitted, don’t allow bulk access/bulk requests, reverse lookups, nor Boolean search capabilities.” So we are talking about this particular line. My request is, since the substance of this line has been challenged and discussed here, to see whether there is ever a different editorial version of this statement possible: for those who defend and for those who challenge. Yes/no?

I do not spend further time here in this room on this very subject. if a group of two will not come up with anything on this one, then

probably this should say. If they can find something that all of us can agree on, then we will modify.

STEPHANIE PERRIN: Can I make a friendly amendment to that? I think what we're hearing is that the other charge of the small group is to address whether not it's within the scope of the EPDP charter. So just answer that and make their recommendation.

JANIS KARKLINS: I would like to concentrate on editorial suggestions.

[MILTON MUELLER]: Again, I'm not clear on what we're voting on here.

JANIS KARKLINS: We're not voting.

MILTON MUELLER: Okay.

JANIS KARKLINS: I will try to avoid voting [inaudible]—

MILTON MUELLER: So I'm not clear on what we're deciding. The current language, to my mind, represents a significant compromise. We thought that we were getting a strict prohibition on bulk access, wildcard

requests, and reverse lookups. Now we have a phrase in there that says, “unless otherwise required or permitted.” We’re willing to accept that. So that’s a huge a compromise.

Now, the question is, do we get rid of that prohibition completely, as Brian seems to be proposing, or do we not? If that’s what we’re discussing, I know what we’re doing. If it’s something else, let me know what it is.

JANIS KARKLINS: Yesterday, we discussed this line and we were and there was a clarification on why this first part of the sentence was introduced: in some contracts, if I recall correctly, these type of things are allowed already today. Then the contracts need to be changed if that is not compatible with the GDPR.

I’m not asking to vote on anything. I’m simply asking to … I’m not asking to vote starting with [that]. I’m asking only [inaudible] two groups who [inaudible] on the biggest difference of [inaudible] to get together and to see whether any change could be introduced.

So they heard you saying that, for you, this text on the screen represents already a big compromise. So you heard that. You heard that. If they can propose something that the team would be able to accept, then we will change it. Otherwise, we will stick with the proposal because prevailing opinion in the room here is that this practice should not be introduced in SSAD.

Brian and Georgios and Hadia. Apologies. Maybe Hadia before Georgios.

BRIAN KING: Thank you, Janis. I really admire Milton's rhetorical style. We don't have anything that is being taken or compromised on now. So the brand new policies [is] the brand new SSAD. So he's not compromising on anything that he has or giving anything away. We're trying to decide if these types of searches are going to be explicitly prohibited in the SSAD. If it's not within our charter to talk about those kinds of searches, then we can't explicitly prohibit that.

That seems to be a real sticking point, so please, can we just delete A and move on? All this is talking about is the types of queries that one could submit into a system that would then evaluate them. So I have a real hard time understanding the harm here. This isn't saying that anyone is going to access to any of this or that any data subject's rights will ever be impacted here. It's just, can you ask the question this way? Thanks.

JANIS KARKLINS: Deletion always is the method of how to resolve issues. This is sweeping it under the carpet. Sometimes it helps in the short term. In the longer term, that may be a difficulty in general. So all I'm suggesting is to please give it a try. Maybe they'll say the best way is to delete. That is the option we may here from the group of two.

Georgios?

GEORGIOS TSELENTIS: Good morning, everybody. Georgios Tselentis from the GAC. I think we're in a phase where we're not productive for this L.A. meeting. I think we are down a rabbit hole. If I can make a suggestion here, as you said, there were some people saying that this already performed by European ccTLDs. Under some circumstances, I asked already my colleagues to check under which circumstances, and, if it is legal, how they made this analysis. So what I suggest is that we post this discussion and we get a more informed decision about the [effect]. Let's keep it here because I don't think we will go in a productive way to either decisions here. So that's my suggestion.

JANIS KARKLINS: Thank you. This is what I'm trying to do to stop this discussion. People are coming back and raising flags.

Thomas, please?

THOMAS RICKERT: I'm terribly sorry. I do agree that we need to move on. I think that, even if we had this on our plate, it would probably be a suggestion of less relevance. I think we should focus on more important things.

My concern – let me be absolutely clear – we are doing this on the world stage. People are looking at exactly what we're doing. If we're stepping over the line of what we can and can't do, it compromises the legitimacy of the outcome of this process. What I want to avoid is that we end up with our recommendations being discussed in the GNSO Council or even at the Board level and

being rejected, partially rejected, or put on the back burner because we have not followed our charter.

So I think, if anything, we need to probably go back to the GNSO Council and ask for clarification. I'm not even sure whether we can answer this question by ourselves if we are not in agreement. I would have hoped that we are in agreement that this is not within the scope of this EPDP. I'm not saying it shouldn't be discussed. So I'm not talking sides on this one. If Council chooses, they can start a different initiative. But I think we can't do that and we should be very interested in maintaining process as polished or the integrity of this process as much as we can. Thank you and sorry for taking so much airtime here.

JANIS KARKLINS: My ruling would be that we stop the conversation about Sub-Point A on the building block/[query] policy/Building Block L. Since there wasn't agreement in the room on the formulation of Sub-Point A – the majority were in support of the principle of no bulk access, and some suggested that it should be deleted, and some suggested that there should be some modifications – I ask James and Mark, and if someone wants to join in private just to talk further about this, to see whether an edit of Sub-Point A could be proposed for consideration of the group. An edit also may mean that we should [inaudible], as it was also suggested by Brian.

With this, I would like to close this conversation. If Georgios will provide some information from .it, that may further inform conversation. When you are ready – I'm not putting any specific

data on you already – please come back to the team with the solution.

Any other comments on other points Building Block L outside Sub-Point A?

James, please?

BRIAN KING: Thanks, Janis. This is Brian. Just …

JANIS KARKLINS: Sorry, Brian. I'm looking to you and saying James.

BRIAN KING: That's okay. Just a point here. The term "bulk access" appears twice. I guess, notwithstanding what we do with A, I just note that we probably don't need it twice. Thanks.

JANIS KARKLINS: I think that staff took note on this, that we need to clarify because bulk access may have two meanings in the context of our work. So that will be edited at one point by staff in the next version.

UNIDENTIFIED MALE: I think it's taken care. The bulk access is footnoted, and there's a definition in the footnote which refers to the definition that's in some contracts. So I think it's done.

JANIS KARKLINS: The footnote says, “As prescribed in Section 3.3.6 of the Registrar Accreditation Agreement,” that meaning bulk access for the purpose of this.

BRIAN KING: Thanks, Janis. That’s the definition that we can agree to. Thanks.

JANIS KARKLINS: [So you are not sure if that’s in the contract then]. In absence of further requests on Building Block L, I would suggest that we move to legal memos. If you’ll give me 30 seconds to consult with staff.

If I may ask to put on the screen Legal Memo 3, the last one.

UNIDENTIFIED FEMALE: [inaudible].

JANIS KARKLINS: The legal memo on automation.

The method I would suggest to use is the following. This memo covers Question A and Question B. I would say let’s talk first on legal advice given on Question A. Once we collect reactions on that part of the advice, then we go to specifically examine advice given on Question B. Does that make sense as part of the introduction?

CAITLIN TUBERGEN: Hi, everyone. As a reminder to everyone, on Question 3 – the Legal Committee and anyone from the Legal Committee can feel free to jump in if a mischaracterize anything – in short, the Legal Committee was asking whether it would permissible under the SSAD to accredit types of group and then, is it also legally permissible to enable automated disclosures of data? Which gets to what the team was talking about yesterday.

The legal question also noted certain legal safeguards that would be in place that the team drafted to see if that would help in allowing the automatic disclosure data or accrediting of groups, of parties.

At a high level, the legal memo notes that it would be difficult for SSAD to meet certain exemptions, which would therefore limit automatic access or disclosure to situations where there will not be “legal or similarly significant effects for the data subject.”

There were some notes that I believe Margie alluded to early, that there may be situations where automatic disclosure could be permissible if, for example, it was a legal entity and not a natural person and didn’t involve personal data. But, generally speaking, the automatic disclosure of personal data is not recommended.

I’ll also note that, with respect to the first question about defining specific types of categories, the legal memo did note that it could be possible to automate the process to authenticate persons making the request or the people and that it might be possible to automate different aspects of the request process. But in terms of

automating the balancing test under 61F or automating the disclosure of personal data, that seems to not be recommended in this memo.

JANIS KARKLINS: Thank you, Caitlin. The floor is open for any comments. Brian, you have – no, your flag was up already before we started this.

BRIAN KING: How convenient. I think one point that I would like some additional clarity on is – the concept that we're trying to tease out here is the automation of the disclosure of data. I know that much of the jurisprudence I've read about automation in GDPR is around automated decision making about the data subject based on their data. It might seem to be a fine point here, but the law and a lot of the jurisprudence that I've read and some of the things that Byrd & Byrd have cited here talk about using a data system somewhere to make decisions about the person: to approve or deny them a mortgage or make a decision that somehow impacts their legal right.

The idea behind GDPR was that that shouldn't happen based purely on automated processing of the data that's stored about a person. That's not exactly what we're talking about here, so, again, it seems to be a fine distinction. I think it's probably worth teasing a bit more, doing some more research, or looking into some more … We can get a little bit more clarity on our request about what specifically we're looking for here because we're not looking to make decisions about the data subject with this data.

What we're looking for is the ability to consider automating whether the data can be disclosed. I hope [that was clear]. Thanks.

JANIS KARKLINS: Thank you. Hadia?

HADIA ELMINIAWI: I will take actually the recommendation they provided as it is. As it says, fully automating decision-making without having any kind of human intervention is not deemed legal. But, again, it doesn't have to be like that. We could have automated decision-making, and then we could have a human at the results. Here you [break] this entirely automated system without any kind of human intervention because you actually have a human that is actually looking at the results of the balancing test.

So that would be my suggestion to the group: to look into the possibility of having an automated decision-making. Then, after the decision is done, you have a human looking at the results and deciding whether to go forward with it or not.

Alan yesterday walked us through the process that he actually goes through to make this evaluation. I think to automate this whole process and not to take the decision from you, to automate all those texts that you needed to go through and all those [inaudible] that you needed to go through is a good thing. In the end, we get a human looking at the results and accordingly deciding if eventually the data is going to be disclosed or not. So that would be my suggestion to the group. Thank you.

JANIS KARKLINS: Thank you, Hadia. I think next is Margie.

MARGIE MILAM: I think it's an overstatement to say that it says that automatic decisions are not possible. So I think we need to delve down into what Brian was talking about: whether the disclosure itself leads to an automatic decision that would be problematic.

From my perspective, when the data comes back to the requester, the requester has to look at it. That's a person. It has to determine whether they're going to either send a cease-and-desist letter or initiate some sort of takedown request, if it's a phishing related event or malware. So that manual intervention actually takes away the issue that is raised by Byrd & Byrd.

So I just want to point that out: they're not saying you can't have automated processing, but, if the decision is automated and doesn't involve a manual step, then there may be a problem. So I agree that maybe Hadia's approach might be something we explore if there is still a concern, but I think I agree with what Brian said: we really need to understand that, in this context, the disclosure itself doesn't lead to a decision affecting the individual.

JANIS KARKLINS: Thanks, Margie. Stephanie, please, followed by – no, Stephanie. First you, Alan.

STEPHANIE PERRIN: Thank you. I look forward to us addressing these issues on a legal basis rather than a group basis. But since we're not there yet, let's look at three hypotheticals in Brian's scenario because, first of all, the automated decision-making principle dates from '91, again, with the earlier directive. It was in there to stop, for instance, a government throwing somebody off unemployment insurance based on the primitive computer tools that we had at the time.

Now, with the new one, I would argue the reverse – you'll be surprised at this – to what Brian was arguing: the interval between Alan handing the data over to Brian and a direct impact affecting the legal rights of the individual has gone down to the nanosecond level.

So, taking my three proposed hypos, we have a law enforcement request, where the decision to hand it over has turned it over to an organized crime investigation that Chris is running. The second hypo would be a trademark violation hunt on the part of Brian's organization. The third, of course, would be an anti-malware thing that's being operated by a private sector security organization.

Now, that can lead instantly to being on a blacklist, which has a direct impact on your use of what would normally be a public utility communication system. So there's direct impact on rights within nanoseconds of handing it over. And don't forget that, were we following the procedural stuff that Alan laid out the other day, the decision that he's got to be making provides legal grounds, the legal basis, for handing it over.

So you're [inaudible]. You [inaudible] can do this.

JANIS KARKLINS: Alan, please?

ALAN WOODS: Thank you. I can't follow very much extra on that. That was exactly what I was thinking. I think the important part here is that our release of that data – we are the tipping point for that decision. Again, throwing off a technical aspect, I do think that the legal advice is clear, and I understand, again, potential pushback. But [plus-one, Stephanie. Definitely].

JANIS KARKLINS: Thank you. Mark Sv?

MARK SVANCAREK: Alan laid out a process that had many steps. I had assumed that, if you wanted to automate any of those steps, if he felt it was defensible to do so, he would be allowed to do so. And, if he chose not to automate any of those steps because he felt it was indefensible to automate those steps, then he was also allowed to do so. So I hear what Hadia is saying, but I assumed that Alan always had that right to do that and would make that choice based on his business requirements.

Is that …. Yeah, please.

ALAN WOODS: We were probably on a completely different page on that one because it's not the whole point of the SSAD to remove that choice of us to be able to take that eyes-on approach. You're saying this is an automated way and it should be done in automated fashion because we wouldn't be making that decision. What you just said there I would agree with, as is, if we keep an eyes-on on that at our behest based on our business, then yeah. That's the whole point of this.

But …

MARK SVANCAREK: Sorry, [Mike]. I thought the point of the SSAD was to automate as much of it is possible – theoretically all of it if possible – but what I was hearing Hadia saying was, couldn't you augment part of your existing process with it? I was saying, well, I already assumed that he was going to augment some portions of it as he felt comfortable.

So, if we're proposing something that is less than automation, I don't see why that's controversial or anything like that. You know what I mean? If it's fractional automation, that seems uncontroversial.

ALAN WOODS: I'm loathe to intervene because there's people in the queue, so apologies. But, yes. But I think what we're getting to at that point is, if [inaudible] value of creating this exceptionally large system, at the end of the day, it could be what we would do normally.

MARK SVANCAREK: That's not quite my point – no, no, no. I understand. What I was saying is I didn't feel like it had advanced the conversation. I'm really terrible at this, aren't I? Okay. Well, thanks.

JANIS KARKLINS: No. Let's listen to the opinion of others. We have now Ben, Milton, Volker, and the line continues. Ben, please?

BEN BUTLER: Thanks. I just wanted to flag that, in our review of this memo, specific to the questioning, there was an idea that came to us in relation to Item 1.12. This is to do with how it might be possible to have an automated system that is not a decision based solely on automated processing. We've talked about the possibility of some sort of AI. I hate to use that word because I don't believe in it. But we've talked about designing a system that has a machine logic built in to make the decision on whether to disclose the data.

Byrd & Byrd goes onto to say, instead of that, the SSAD could publish the categories of requests that will be accepted. These would have to be categories as I interpreted that don't have a legally significant implication on the data subject and so isn't going to wind up in them getting arrested or hunted down and shot in the streets.

Let's say the desired effect is to be able to stop a phishing attack. People don't get arrested for phishing attacks anymore. It's just whack-a-mole. That's what these kinds of things are.

So, in that limited set of categories that are not legally significant – we can define what those categories are – the SSAD publishes what those categories are. It asks the requester to confirm that these meet the relevant criteria. If that confirmation comes back, at least by my interpretation, this is no longer a decision based solely on automated processing. Then the data can be disclosed in the automated process.

I'm being specifically focused on the types of things that security practitioners tend to want to do. They're not after someone getting arrested. They're not after someone getting hunted down or losing liberty or any losing their job or anything like that. They just want the bad site turned off so everyone can go about their business.

I am absolutely not a lawyer. I never even played one on television, but I would love see some sort of discussion, whether now or later, including when we've had time to properly legally digest, on if this paradigm something that we consider that would at least alleviate some of the high-volume stuff that we're dealing with because, realistically, the ones that might involve legally significant loss of life, loss of liberty, are fewer and far between. It's the hundreds of thousands of abusive domains and websites that we are trying to deal with that would make the biggest impact to cleaning everybody's plates: contracted parties and researchers and everybody. Thanks.

JANIS KARKLINS: Thank you, Ben. Milton, Volker, and Ashley.

MILTON MUELLER: My initial point is simply that we have – whether you can quibble about the specific applications about this legal opinion or not – a clear warning flag regarding risk. If the conclusion of this is that Article 22 prohibits decisions based solely on automating processing, which have legal or similarly significant effect, it is likely to be difficult for SSAD to meet these exemptions. It needs to be structured so that it does not fall within the scope of Article 22. I think we just need to accept that. Even people who don't like that need to just say we can't put ICANN or SSAD at legal risk of being challenged, so we need to really carefully work around the boundaries of that.

Now, I think what Ben said was indeed trying to respect the decision and say, can we carve out particular type of requests? I think that may be possible for a very, very carefully defined set of requests.

In terms of legal effect, I think what you have to talk about with your high-scale phishing attacks is not loss of life or liberty. It's loss of a domain. That's an effect. If you're talking about disabling or taking away domains based on that, you're probably in the world of legal or other effect that should not be automated. If you're talking about just knowing further information about who's running a botnet or about who's doing the phishing, I think that that might possibly qualify for an exemption. It's something to be explored.

JANIS KARKLINS: I also hear Milton agreeing that we may think of certain types of queries potentially that would fall outside this legal risk.

Volker and Ashley?

VOLKER GREIMANN: I'll cut my response shorter by half. I, first, agree with everything that Milton said. One point I do want to make is that internally we're basically free, assuming that the decision-making process remains with the contracted parties, to design our systems any way that we like to do. If we want to automate parts of the system that leads up to the decision-making, where the decision-making would only have between two or three options and then click a button and the answer goes out, that's our prerogative because we base that on our risk management and our [inaudible] questions.

We might even go far to say that, for example, law enforcement [inaudible] jurisdiction may get a fully automated system based on who they are and what they represent with their request if we feel comfortable with that [inaudible].

I do feel uncomfortable in prescribing that as the norm or as a requirement because that basically takes away our decision-making power and our risk assessment. Also, that also infringes on the right of the data subject. For example, law enforcement has a legal right to make a certain request, and we do not have any determination right to demand that request. The [automated] response can go out automatically, but in all other cases where we have to make a determination, that determination has to be done by a human at some point because I don't feel that, as Ben said, AI is quite there yet or even possible.

JANIS KARKLINS: Thank you, Volker. Ashley, and Matthew is next.

ASHLEY HEINEMAN: Ashley with the GAC. It sounds like we're all somewhat in violent agreement and that we recognize that full automation is not going to be possible and it's recognized in the legal memo.

But I think we also agree on that we can automate as much as we possibly can and that's what we should be striving for. For areas that can't be automated, I think we need to add on to that standardizing as much as possible.

I think where we're probably not quite at agreement yet is if we could keep this as a responsibility of the decision maker. Once again, just to sound like a broken record, if the intent here is to streamline a process and to keep it as efficient as possible, having a single decision maker or at least a single entity responsible for decision-making I think permits an automated-as-much-as-possible approach more likely, as well as a standardized [one] when the human eyes are necessary. So that's that. Thanks.

JANIS KARKLINS: Thank you, Ashely. Matthew followed by Alan G.

MATTHEW CROSSMAN: I strongly agree with a lot of what Ashley just said. I think, to put a positive spin on this, the opinion is very clear that we need human involvement in the actual decision to disclose. I think it would be

productive if we as a group could reach that sort of agreement going forward in our discussions about this topic.

But what I think that leaves open, which Ashley has flagged, is a lot of opportunity to automate the input into the system, everything short of where we are making that decision about disclosure. I think we could have a lot of that on the table and see whether there's some ways that we can find efficiencies for the folks who are trying to request this data and access this system so it makes your lives a bit easier and potentially makes our lives a bit easier.

I think it's a separate question then on whether building such a system that just gains those efficiencies is worth it, but I think that is a discussion that we should have.

So I think maybe the most productive thing we could do coming out of this memo is agree with that distinction that human involvement is going to be needed in the actual decision-making process of disclosure but that we could discuss going forward how we might be able to automate some of the input into that process. Thanks.

JANIS KARKLINS: Thank you, Matthew. Alan G followed by Chris – no, Chris is not … Then Margie. Alan, go ahead.

ALAN GREENBERG: I'm hearing different things. Matthew said we should come to the conclusion that we cannot automate anything, and I thought I heard Ben suggest and Milton – [no?] – that we cannot automate

the decision. And I thought I heard Ben suggest that there may be some cases where we can automate the decision. So, again, we're at somewhat different odds here.

A comment on one of Stephanie's comments of, if we get the information, we may put someone on a blacklist instantaneously. I would have though it's just the opposite. The information may stop us from putting them on the blacklist. The default is to put someone on the blacklist. In fact, we are blacklisting a lot more people now because we don't have information that we might have otherwise, or at least larger groups of people.

I agree with everyone on AI, by the way, but I find it curious that we're willing to let AI control very high-speed chunks of iron on the freeways, which can plow us down, but not for this. I just find it curious.

I think with any solution we pick, no matter how much automation of the decision that we may allow in some cases, we are always going to have to have what I was calling the other day the escape hatch: the ability for a contracted party saying for certain classes or maybe everything, "I insist on having the decision myself." So we're always going to have that level of granularity, even if we allow some decisions automatically. Thank you.

JANIS KARKLINS: Ben, do you want to clarify what you said or did you have further question?

BEN BUTLER: Just really quickly to clarify. This is just me putting my hat on as operational security and hopefully to alleviate some of the concerns. The thing about abusive domains that is the first question that security needs to answer, whether they're a third party or [me] working in the abuse department at a registrar is, was this domain name maliciously registered as part of the abusive activity, or is this a compromised legitimate registrant/data subject? One of the easiest ways to start to unravel that is to learn who it is and what their registration data is.

So the reason that a security researcher would want this data is to be able to look at it and say, "That's clearly blatantly false data, probably malicious, and also is the same false data of these other bad guys that we've seen in the past." That's the added value that they provide.

If it's a real data subject, a legitimate person, then the conclusion that comes out of that is, okay, it's probably not them, so at this point now we just want to initiate contact with either their host or their register or their data subject themselves and say, "It looks like you may have been hacked." We're not talking about an automated add to a blacklist that will loss of connectivity. We're talking about trying to protect the legitimate people while identifying the bad, automated, terrible, bulk registrations that are clogging up the pipes. So this is literally, I think, a protection of a data subject's attempt, rather than the other way around.

In those very specific, finite set of circumstances, possibly – again, I just want to flag this for discussion after we've all talked to our lawyers and slept in our own beds and all that kind of thing – maybe … Because so far we have not talked about the possibility

of just a basic challenge in response. “Are you sure this is one of these super green light categories? Are you super-duper sure? Check the box again. Fine. Here’s your data.” It would all have to be tied up with a pretty bow of accreditation to know who these people are and if they have a reasonable expectation of knowing what they’re talking about.

JANIS KARKLINS: Thank you. Margie is next.

MARGIE MILAM: I think what Ben is talking about is what makes a lot of sense. We’re talking about identifying categories where there could be automated decisions or close to it if you need confirmation – that sort of thing.

The other thing I wanted to point out that Caitlin mentioned from the memo is that Byrd & Byrd did identify other categories that could also fit in that world where you don’t need to have a more manual process, one being that the legal person. That’s an area that you could automate. So I think that’s something we should also be considering as part of this process.

JANIS KARKLINS: Thank you. I have many people still on the list: Hadia, Stephanie, Mark Sv, Brian, and [continuing]. Hadia, please?

HADIA ELMINIAWI: I just wanted to point out that automation to a great extent ensures compliance with GDPR because the decision is based not on a human assessment but on a set of rules carefully put together. From the memo, it's clearly obvious that we need to have some kind of intervention at some point. That point would be looking at this decision in the end.

Looking at what you presented to us, Alan, yesterday and taking from Ben talking about AI, I think all what you described yesterday could be automated from start to end while putting a bit of artificial intelligence into it. Again, there needs to be a human intervention, and we all acknowledge that. If the decision is made and you look at the decision, that's a kind of human intervention.

Again, Ashley said something that I find very important, and that is that that final human intervention, done by a single entity, is much better. But then that's again to be considered. I'm totally for exploring what Ben was talking about: exploring cases where actually full automation of disclosure of data would be possible.

JANIS KARKLINS: I want to suggest that we close the speakers' list for the moment. Those flags that are up will have the floor. But please do not raise any more flags because we will go to the coffee break and then we will come back and then we will continue. Okay?

Stephanie is next, followed by Mark Sv.

STEPHANIE PERRIN: Thanks very much. Two points I wanted to make, following Ben's discussion of his use case scenarios. One of the reasons we want to focus on the legal basis as opposed to the group is that not all security investigations are created equal. The type of scenario where he is discussing actually protecting the individual whose domain has been hijacked and is spewing malware is a disclosure potentially for the benefit of the individual. You can make a pretty good argument under data protection law that that could be automated, right?

I get a worried look from Alan. But it is very important to look at the legal basis when you're judging these decisions. So we should get there sooner rather than later in my view.

Secondly, one of the reasons we like the independent data trust model – I'm going to just start advertising this, folks, because I don't think people even understand we've done a lot of work on this – is that you can embed a trusted security researcher rather than fiddle around with, is it automated/who are you going to trust? Do it independently. Put somebody that is elected by a board of registrars that they realize is not somebody working for a criminal gang with a security company as a front but is a bona fide investigator. Then they eyeball these decisions at the end because each legal case is going to be different in terms of that balancing test. Thank you.

JANIS KARKLINS: Thank you, Stephanie. Mark Sv, followed by Brian.

MARK SVANCAREK: I almost put my card down because I [was going to say] I agree with Ben, I agree with Milton, I agree with Matt, and I agree with Stephanie. It might not be so very useful. I just wanted to call out the fact that scenario that Ben and Stephanie were talking about was captured in [BC] 1 and we discussed various approaches that can be taken, when is this a contractual thing, when is it just a legitimate interest, and how do you just discern primary victims from secondary victims. So it may be of interest to look at [BC] 1. We didn't get a chance to review that in plenary, but there is something captured there. Thanks.

JANIS KARKLINS: Thank you, Mark. Brian?

Okay. Marc?

MARC ANDERSON: Thanks, Janis. I actually wrote some stuff done during this conversation. This is the first time I did that all week. So take that for either my mind failing me or, as I think, more a statement of how significant this conversation is.

There were a couple things I thought that were really important to highlight. This is going back to something Ashley said earlier. She said, "Can we accept that full automation is not possible but that some automation is possible and that, as a principle, we should automate where possible? And then, as another principle, we should say, where it's not possible automate, we should strive to standardize?" I wrote that down because I thought those were really good points that we should consider as principles. If we

agree that full automation is not possible but there are places where we can automate, then in our SSAD system, let's do that. And then, where not, let's standardize. That seems very much in line with what we're tasked to do. Those seem like very good principles that we can take out of this legal memo.

Changing topics a little bit—

JANIS KARKLINS: Sorry, Marc. Could you stop here? You will continue. On what Marc just said, is there anyone in disagreement with that?

Okay—

UNIDENTIFIED SPEAKERS: [inaudible]

JANIS KARKLINS: I see that, on those two statements of principles, we can agree. That will be certainly captured in the 1.0 draft.

Please continue, Marc.

MARC ANDERSON: I don't know. I feel like I should just stop on a high, so I'm going to …

JANIS KARKLINS: No, no. You should come to my place and run the show.

MARC ANDERSON: I do want to point out two other things from the legal memo that I think are important. One is that contracted parties are controllers for the purposes of disclosure – I think that was one of the key items from the memo – and also that contracted parties retain liability in the SSAD. We haven't got there yet, but I think those are key points from the legal memo that I wanted to highlight for everybody.

JANIS KARKLINS: Thank you. Thomas?

THOMAS RICKERT: Thank you. All this agreement in the room makes me tipsy. So we finally managed to turn this into a love fest after all. That's great.

I just have a question for confirmation with the automated decision-making. You let me know whether I'm on the right or on the wrong track. I think what we hear is that what we can't do and shouldn't be doing is throwing information to a black box and some sort of decision comes out of that. But we can do is – this is the example that I mentioned yesterday – is, when we have a security researcher investigating a phishing attack and the parameter is always the same, that we do a manual balancing test and that we apply the results of their test to exactly the same cases as we can. Right? Because, from one of the statements, I though there were different views on the possibility of that. If we're aligned on that, we have another point of agreement to add to the list. Great.

JANIS KARKLINS: Thank you, Thomas. Chris, are you seeking –no? Matthew? No? Okay. Then Alan – no?

I think we got rough agreement on principles that we would automate as much as feasible and, where automation is not possible or advisable because of the risk, we would try to standardize as much as possible. So that maybe is a takeaway from this conversation.

Hadia, you … Yes, please. But you will be the last one.

HADIA ELMINIAWI: I'm just responding quickly to Thomas. I just want to elaborate that it's not a black box. The decision maker should always be able to explain, even if it's automated, how and why the decision was made. So we're not talking about black boxes. Thank you.

JANIS KARKLINS: With this, I would like maybe to make a little pause. We would take a coffee break for about 20 minutes now and then we reconvene. But please be aware that this is the last coffee break before the end of the meeting. We will then plow through to 2:00 P.M. and then we will draw this meeting to an end. Coffee break. 20 minutes. We will revisit then Question B.

The issue of Question 2 is on the balancing test, [which] replies to Question B of the Byrd & Byrd memo. Any thoughts? Any reactions? Caitlin, you want to say something to start?

CAITLIN TUBERGEN: Thanks, Janis. What you'll see on your screen in Paragraph 2.2 may look familiar because it's essentially the stuff that Alan Woods went through yesterday and how he personally performs the balancing test. You'll notice the four steps outlined there. First is to assess the interest which the processing [meets]. Two is to consider the impact on the data subject. Three is, once those interests have been assessed, to undertake a balancing test. Fourth is to consider the impact of any additional safeguards employed. As a reminder, the legal team did add a list of safeguards to the question so that Byrd & Byrd could take a look at that and answer the question based on those. As you go through the memo, Byrd & Byrd gives advice about how to conduct those four parts of the balancing test.

JANIS KARKLINS: Thank you. Any comments? Any reactions? Chris?

CHRIS LEWIS-EVANS: Thanks. I had a good read of this last night. As many people have said, I think a night in my own bed and without eight hours difference would be helpful. But I think it's quite helpful to call out the safeguards that we obviously sent with the question here. I think in the last few user cases we've made a couple of adjustments. It said that this is very helpful. I think my reading of this is maybe this is something, a task, that we probably need to carry out: a more detailed look into the safeguards that've highlighted across all the user cases and come up with a definitive list that would help the contracted parties to perform that

standardized and consistent balancing test. That's my [inaudible]. Thank you.

JANIS KARKLINS: Thank you, Chris. Matthew?

MATTHEW CROSSMAN: I agree. I think the analysis here is helpful. I think it aligns nicely with what Alan has already presented. I know we have a lot we want to try and cover today, so my suggestion to get to a next step, unless anyone has any strong feelings about this, is we take this guidance, build it into the doc that Alan has already prepared, and create one comprehensive, hopefully simplified guide to the balancing test and then circulate that to the group to get comments and take that as our next step here going forward.

JANIS KARKLINS: So I understand you volunteer.

MATTHEW CROSSMAN: Yes.

JANIS KARKLINS: Any other comments, reactions, or reflections?

If none, then we can move to the next memo, and that is Memo # 2, right?

UNIDENTIFIED FEMALE: [inaudible]

JANIS KARKLINS: Question 4. If you will pull it to your screens, I will try to pull it to mine.

Question 4 is, can the data controller rely on Article 61C of GDPR to disclose personal data to law enforcement authorities outside the data controller's jurisdiction? I think that was from the use case that Chris presented. Caitlin, would you like to introduce that?

CAITLIN TUBERGEN: Thanks, Janis. Janis just introduced a question, but this is essentially about the lawful basis that a law enforcement authority outside the data controller's jurisdiction can rely on. The short answer – again, please feel free to weigh in if you believe I'm misinterpreting – is, generally speaking, law enforcement outside the controller's jurisdiction cannot rely on 61C as a lawful basis. There are some exceptions noted in the memo. I believe there's some specific treaties noted.

As you scroll down through the memo, the Legal Committee also asked if 61F could be relied on. Byrd & Byrd went through all of the six lawful bases and weighed in on which unlawful bases could be used.

If you scroll down to Paragraph 2.2, you'll note that 61A is not a basis that can generally be used. Byrd & Byrd also notes that 61B

is generally a lawful basis that can be used. We already went through 61C. In very rare situations, 61D may be used.

The last part of the memo goes through, if the law enforcement agency were to rely on 61F, how that can be done. If I may put Thomas on the spot, I believe that, Thomas, you were the one that suggested that we ask these questions to Byrd & Byrd. Maybe you can explain why you thought that would be useful for the team's work.

THOMAS RICKERT: On the law enforcement 61F thing, right? Just you want me to focus on that one?

The reasons for my request to answer the questions is that, typically, law enforcement in Europe must have an explicit legal basis to ask for data and let's say in the telecommunications they actually sometimes have that. Or, in the procedural codes, you might have a legal basis for asking for data. Then the contracted party can return data based on 61C for filling a legal obligation to disclose the data.

Now, that only works – that's part of the question – according to legal literature, when there is a European statutory legal basis based on which law enforcement can ask the question. So the question is then, how do we deal with non-European law enforcement requests to contracted parties? Because they don't have a legal basis that would work under 61C. So the first half of the question is, can we deploy non-European legal bases so that the contracted parties can return data in response to those

requests based on 61C? Or, in the absence of that, can contracted parties disclose the data based on 61F in the absence of the European legal basis or the law enforcement authority to base their request on?

I guess the reason why we've asked that explicitly is that there is, in my view, a value judgement in the way the GDPR was drafted. So they were requesting a law to request the data. If we have no other alternative than 61F, than an interest would be sufficient. So we would basically say, let's say, a German law enforcement authority asking a German registrar to disclose data needs to have an explicit legal basis, a law, to ask for the data, while some non-European law enforcement authority can ask for the data based on 61F, just claiming they have an interest in the data. Therefore, the question is whether that mechanic is potentially blocked, particularly since 61, at the end of the catalogues of 61s, explicitly stated that public authorities can't use 61F as a legal basis for their own processing when performing their core functions.

This is basically the question that we asked, and I tried to offer a little bit of reasons why we asked it. But I think you're going to disclose to us now what the response from Byrd & Byrd was.

JANIS KARKLINS: Thank you for clarifying. Chris, I think you wanted to intervene.

CHRIS LEWIS-EVANS: Yeah. Thank you. As you said, it's obviously – yeah, sorry. Other Chris, Chris. As you say, this covers the two users cases that I

submitted. I've had a good read of this advice, and I am reasonably happy, not certain at the moment, that we don't need to do any changes to the user cases that I presented. So I believe that the advice that is in this memo matches already how I've detailed the processing activity that would take place for law enforcement people inside and outside. So I'm fairly comfortable with that.

I'm looking at Thomas, who's not shaking his head in violet disagree. So I think it's a good memo and a good clarification that Thomas has just highlighted.

JANIS KARKLINS: So then I understand that this memo could be used in formulating further texts in the building blocks. That will turn into at one point into a draft policy recommendation.

Alan, you're next.

ALAN WOODS: Thank you. I just wanted to point out one thing, which was a learning moment for me as well. I just wanted to point it out, which is interesting because I'm going to have to apply it now going forward as well. That was in relation to the MLAT. I was not aware that, if there is an MLAT that applies, I should not disclose. I must refuse to disclose that because I should refer to the MLAT. But I'm just reading and you can please clarify that.

CHRIS LEWIS-EVANS: I read that, and I didn't think it was very clear in the letter, actually. What that should be is, if I sent you a court order from my jurisdiction, you should not react on that. You should say, "Go and get an MLAT."

[ALAN WOODS]: Yeah.

JANIS KARKLINS: Next in line is Matthew.

No? Okay. I understand that no further requests – no. Alan. Alan G, please.

ALAN GREENBERG: I'm just curious about the last one. So, if an MLAT exists, you have to use it. If it doesn't exist, then it's a judgement call on the registrar or registry whether to release the data based on the merits of whatever the thing is that's presented to them.

CHRIS LEWIS-EVANS: I've obviously not explained that very clearly then, Alan. I cannot send a court order, a U.K. court order – I'll stick with Alan; no, I'll go onto Mar[c] for a change, rather than pick on Alan – to Mar[c] in the U.S. because we have an MLAT process with the U.S.A. So I would have to go through the process that is, which is effectively going through a couple steps to then go and get a local court order within the U.S., which will then be served upon Mar[c].

If I wanted to ask Mar[c], which is not compulsion – it's a low request and you have the 61F issues – then I can still do that, only if I am trying to force him to do something – sorry; compel, not force. That's a different time. So it's only if I'm trying to use my compulsion method that I need to go through the MLAT process.

If there's – I think they've highlighted it – no MLAT process, then you pretty much have to use other methods which becomes difficult.

ALAN GREENBERG: Essentially, if there's no MLAT process, you're presenting a nice piece of paper called a court order in your country, but it doesn't have any legal impact. It may still impress them and cause them to give the information?

Okay.

CHRIS LEWIS-EVANS: And you lose the 61C, effectively.

JANIS KARKLINS: In that case, we can draw this conversation to conclusion if there are no further requests.

Stephanie?

STEPHANIE PERRIN: Just a question. How does Jack feel about the guidance that we ought to be offering on this? Because it seems to me the legal basis they [seize] have gone out the window. If you don't have an MLAT, you're out of luck. Or you should be out of luck.

CHRIS LEWIS-EVANS: No, that's not what I said. It says explicitly in this document we can rely on a 61F outside jurisdiction. If we want to rely on a 61C, we're still going to have a balancing test. Then we have to go through the legal process. If there is no MLAT, we cannot rely on a 61C.

STEPHANIE PERRIN: Okay. Maybe I wasn't being explicit enough. If I were to a balancing test under 61F for an outside law enforcement where my constituents don't have any constitutional rights or due process rights, I don't think it would pass the balancing test. It depends on what they're asking for, yes. It depends on the specific case, yeah.

Okay. So we potentially agree on this in some instances.

I don't feel the love here.

JANIS KARKLINS: I think we need to stay focused on our tasks. These seem to me to be conversations that are good to know but we don't necessarily need to know.

Any further specific comments on the memo on Question 4?

If none, then let's revisit the first memo that we started to talk about yesterday and didn't finish concluding. They may not be sufficient. People were not ready to talk about it. Once again, it covers two questions.

Caitlin, will you help me kickstart and formulate questions?

CAITLIN TUBERGEN: Thank you, Janis. As everyone might remember, Leon introduced this memo yesterday. The team has a robust discussion about joint controllership and what the effects of that would be in terms of liability.

However, some team members around the table had noted they hadn't had time to read the memo yet and had requested that we bring this discussion up at a later time. We just wanted to see, since everyone was here, if anyone did have the chance to read the memo and if they had anything to add from the conversation from yesterday, or if we instead need to postpone the discussion to a later plenary meeting.

JANIS KARKLINS: Thank you, Caitlin. So it's an open-ended question. Is there any desire to continue the conversation on top of what we had yesterday when we were dwelling on joint controllership and then had a rather robust and lengthy discussion. The floor is open.

Okay. The answer is obvious. In that case, if we are not willing to continue with this conversation for the moment, let me maybe suggest the following. I will try to summarize how I see where we

are and then what would await us going from here to Montreal and after Montreal and then see whether any elements of what I will try to summarize would create violent disagreement, including on the proposed next steps going forward.

Actually, I have a reasonably good feeling that we have embraced in principle this hamburger model and that we can continue our activities in further developing building blocks of the model that would stand independently by themselves, no matter what type of model we would choose at the later stage when we will have additional information either from the European Data Protection Board or further clarification from Byrd & Byrd on legal issues if we will decide to pose further questions. Those building blocks would be, I'd say, an integral part of any standardized system that we may end up agreeing on.

I would try also to talk a little bit about the process because that is important to capture and understand or for me being on the same page on that. When a requester sends out or formulates a request, the parameters of which we have no discussed yet – or, if we did, they are described rather vaguely in, if I'm not mistaken, Building Block A, right? So what type of the information the requester needs to put in in a standardized way is a template of a question that we still need to develop.

On the requester's side, the big question that we discussed, and the building block of accreditation, is that we need to continue our conversation. I think we, in principle, agreed that the minimum that an accreditor would do is to confirm through the process determined by certain criteria identity of the requester, being an individual or organization, and would send a signal to the system

that the accredited person or entity has a good reputation and is what the entity claims it is.

Elements of this accreditation need to be further worked on. Alex and Milton volunteered to continue working on elements of accreditation based on both inputs that have been put forward. All the systems of accreditation need further discussion and development in terms of auditing and the accrediting and all the elements that we discussed yesterday.

I hope that, in about ten days, we would have additional inputs from the small group and that we can continue discussing this accreditation building block in further details.

Stephanie?

STEPHANIE PERRIN: Just a question. Perhaps it's premature, but have we agreed on a definition of accreditation that limits the scope of the accreditation to identity accreditation? Or are we working on that?

JANIS KARKLINS: I think we agreed that accreditation at a minimum needs to confirm identity and see whether the accreditation system could provide also any further service.

STEPHANIE PERRIN: Well, the reason I bring this up is that, in my view, it's at a maximum because, if you go beyond identity accreditation – in other words, into capabilities and authorities – then you get

yourself into the certification procedures from Article 42 on. That's a whole other process. Identity accreditation is pretty easy. Anything else is very difficult and possibly impossible.

So what's the scope of that little group? Maybe my worthy colleague on my right needs me to join.

JANIS KARKLINS: Alan G, Alan Woods afterwards, and then Alex.

ALAN GREENBERG: We spent a lot of time the other day on a flipchart that seems to have disappeared, coming up with other possible benefits of accreditation. We also had a significant discussion saying, since the articles in GDPR that talk about it talk about accreditation by the state and that it's not something that's likely to happen here. But we discussed the possibly of doing something akin to those standards and hoping that it would be accepted by the Data Protection Board as a best efforts given our unique situation addressing multiple countries and spanning large areas.

So I don't think we decided that it is identity only and that that is the only benefit that we might get out of it. So I think we are quite far from that position at this point.

JANIS KARKLINS: No, no. Certainly we haven't reached the end of the conversation on accreditation, but we acknowledge that that would be minimum. There was also some question marks on whether the

accreditation would not be too bulky and expensive, if that makes any senses. But at least we had a solid basis to continue that conversation and see where that would lead or to what agreement that would lead.

Alan Woods?

ALAN WOODS: Just in relation to what Stephanie was just saying there, I think what you said is absolutely right, but the Article 43 or Article 43 – or is 34 or 30? There's one you're talking about. I should know it by now. I don't think we should rule that one out, absolutely, because that would be out of our hands because, yes, it's utterly complicated – the certification aspects – but the benefit of having the Article 42 or the Article 43 would be specifically that we can then say we can expect that they are adhering to a certification that implies that their processes are in line with data protection requirements in the European Union and that we don't have to make that call. We can just follow that.

So I think we can keep that in as a concept, noting it's an exceptionally high bar. I was talking to Georgios earlier, and that's the gold standard. But I wouldn't rule it out.

JANIS KARKLINS: Next was Alex.

ALEX DEACON: Thanks. Hi. It was my takeaway from that discussion that we needed to consider items beyond identity and pulling concepts in Article 40 [.]Code of conduct, Article 42 and 43 I think was key to ensuring that it was actually useful in terms of accreditation to those that would be processing the requests.

So my takeaway was that we would talk about the identity piece but also flesh out what additional useful things would be required based on the discussion we had on Monday or whenever that was. So that's my plan.

JANIS KARKLINS: Thank you. Mark Sv?

MARK SVANCAREK: I wanted to further acknowledge Stephanie's point about certification. Just as an FYI, Microsoft's privacy and regulatory affairs team has been thinking about that distinction for a while. The advice that they had given me preliminarily was that this seemed like it was a good candidate for codes of conduct and accredited monitoring bodies. But they're actually at the commission today, and they're asking questions about certification and codes of conduct, not in the context of this at all but in a more general fashion because they have concerns about impacts on various industries. If the feedback that we get is pertinent to this topic, I will share it. Thanks.

JANIS KARKLINS: Thank you. Milton?

MILTON MUELLER: I think there is something that did discuss about accreditation yesterday. I think we can rule certain things out. One of the proposals – I think Becky described it on the board – is that, in effect, the accrediting agency would be authorizing as well as accrediting. Therefore, once you are accredited, you would make a request to the SSAD and it would be granted, no questions asked. I think we can rule that out. That is not—

JANIS KARKLINS: No.

UNIDENTIFIED MALE: I don't remember having that discussion.

JANIS KARKLINS: No, that's not the understanding. Basically, accreditation would mean that the accredited entity puts the question in SSAD. Whatever process we have in SSAD for examination of that request would not have an element [of] who is asking. We know that who is asking is someone who can ask. So—

UNIDENTIFIED MALE: [inaudible]

JANIS KARKLINS: That was a friendly gesture.

MILTON MUELLER: [inaudible] all accreditation can ever do, but Alex and I will have to work something out. It will have to be both of us, and it will not just be you reiterating your ideas or me reiterating my ideas. We're going to have to work something out because, again, when we were talking yesterday about who makes the disclosure decision, nobody brought up the accreditor, right? So that was considered off the table, I thought at that time. So I hope that that—

UNIDENTIFIED FEMALE: It's off the table.

UNIDENTIFIED MALE: Yeah.

MILTON MUELLER: It's off the table. Okay. So when they talk about the other things the accreditor can do, I'm unclear as to what that is, other than certifying the identity in some way of the requester.

JANIS KARKLINS: We have a conversation that, for instance, accreditation would also entail providing access to SSAD, which means that an accredited agency would give, for instance, a password that would allow a requester to access the system and submit the request.

We also talked about how an accrediting agency would be also examining once in a while the behavior of accrediting agencies if

there is reason to believe that the requester is misbehaving or has misbehaved based on audits that would be performed periodically in the system.

We were talking about how there should be maybe also some kind of process of de-accreditation in case of abuse by the requester who is accredited by an authorizing organization.

We also talked about who then would be those accreditors. WIPO was mentioned as one potential accreditor for the IP crowd, but Interpol or Europol was ruled out as an option for law enforcement agencies.

Then we had a side conversation with GAC members, and we came to a possible model: that each country would have one authoritative entry point of law enforcement that would interact with SSAD as an accreditor. In case of law enforcement, every request would come through that one point. It was mentioned, in the U.S. case, that it's maybe the FBI. In other countries' case, that could be the national authority that would serve that function. We would not know what is behind that organization, but that would be a trusted and authoritative accreditor of law enforcement.

What needs to be decided is what would be possible accreditation schemes for security researchers for the business community. Again, that has not been discussed. We need ideas/models of how that could be organized.

MILTON MUELLER: But I also insisted during that discussion that there would be a channel for non-accredited people to use the [best]—

JANIS KARKLINS: Yeah, as well. So all that needs to be further fleshed out. Hence, all hope is on Alex and you to come up with a workable and scalable solution.

UNIDENTIFIED FEMALE: I would just add, if I may, that I took pretty detailed notes and I was literally just typing them up. I'll share them with Milton and Alex to help jumpstart the conversation.

JANIS KARKLINS: So, on accreditation, Alan G?

ALAN GREENBERG: Just very brief, Janis. You said pretty much everything I would have said and a lot more. There are certain things like authentication, which [inaudible] said checking the passwords, which are natural fits that might work. I think we have ruled out anything where that body would be viewed as the wolf guarding the henhouse, so to speak, that, if they're going to do the de-accreditation, if they're going to do the audits, there has to be a very high level of comfort that they're doing it legitimately and not just protecting their friends. So those things are going to have to be looked at in great detail.

JANIS KARKLINS: Yeah, there should be safeguards in the system, obviously.

ALAN GREENBERG: Yeah. Thank you.

JANIS KARKLINS: Margie?

MARGIE MILAM: I think the other thing that accreditation might do is help establish some of the legal bases. In other words, with WIPO, when they made the presentation in Marrakech, I believe the pilot showed that people could upload their trademarks. So I think it makes it a little easier for whoever is the decider to know that, when WIPO is accrediting a trademark holder, there's some indicia that they do have trademark rights, as an example, because that's been at least uploaded and perhaps checked in some way. So there's a little bit more than just identifying the party.

JANIS KARKLINS: I think we would need to establish some kind of accreditation criteria, which may slightly differ from group to group. If we're talking about user categories or requester categories, I don't like requested groups. I prefer requester categories. Accrediting entities should follow those criteria when they do accreditation so that we're sure that they would do that thing properly.

So that's an accreditation. We – sorry. James?

JAMES BLADEL: To Margie's point, accreditation, I think, has a couple of different layers. First is establishing identity. I think for a lot of folks it stops there. I think it can inherit some attribute of which legal basis you can use. But I don't think what we can then take the next step and say, "Well, because WIPO says that they've accredited you, therefore your trademark claims are valid." Those still have to be reviewed. But at least we can say which door you can come in and that they are who they say they are.

I think we had the Chinese law enforcement example a couple days ago, which is, "I would like to know from Interpol that Chinese law enforcement is Chinese law enforcement." I can tell them to go pound sand after that – probably will – but I still want to know that I'm talking the organization that I think I'm talking to."

JANIS KARKLINS: Yes, I agree. That's the meaning of accreditations. Mark, please?

MARK SVANCAREK: I agree with pretty much everything everybody has said. I had thought of a couple of other examples of authorization that might be attached to accreditations, one of them being, if you are an accredited person, you might get a higher level of volume access. The unaccredited person would probably not be allowed to make n number of calls during a day, whereas an accredited person potentially would have a different threshold.

So I think there's a number of these authorizations that could be discussed, but I thought we had agreed that the whole carte blanche "WIPO says X and therefore you can see everything – I agree – is off the table. If that's not clear, I'd like to confirm that.

JANIS KARKLINS: That is clear, and I believe that that is already an element that we have agreed on.

MARK SVANCAREK: I guess it wasn't clear, so I think, with this discussion, we've made it clear.

JANIS KARKLINS: Thank you. Stephanie?

STEPHANIE PERRIN: Getting back to my original scope question, I guess I just wanted to put on the record that, in my view, this working group and ICANN in general should not in any way be interfering or assisting or working on the certification of different groups, even if they're stakeholders, to reach that higher level of code of conduct review. It's a good thing. Don't get me wrong – a great thing – but they do it on their own dime. Thanks.

JANIS KARKLINS: We didn't discuss – and intentionally – user groups. I think that they are a natural part, and I don't think we need to spend time

trying to identify how many of them. We may revisit the issue once we will be talking further about accreditation: how many accreditation bodies we will have and then for what purposes and how that will function.

But equally we didn't touch the issue of Building Block D that needs further discussion. But, again, that was not seen as a first priority for the face-to-face meeting. Certainly, we will continue working on acceptable use policy during our meetings online.

Then we had a conversation based on Byrd & Byrd's advice on joint controllership, where the decision on disclosure could be made. This was a rather lengthy and robust discussion, where, let's say, a majority of views expressed were related to that there should be one point of discussion making, and that would be ICANN. Another point of view was that ICANN may not be an appropriate decision-making point, and the decision on disclosure should stay predominantly with registrars.

MILTON MUELLER: Janis, I have to challenge. There was no majority in favor of the latter. [inaudible] by stakeholder group. It's perfectly split. I don't see where you got the idea that there was majority in favor of ICANN.

JANIS KARKLINS: Okay. So there were two points of view expressed. One option was that the decision of disclosure could be made by ICANN. Another is that it should stay with the registrars and registries. We came to some kind of feeling that, if certain conditions could be

met, then the compromise/solution of where this decision is made could be in the very clearly defined and very detailed joint controllership agreement, and proper policy [would be] put in place and enforced. In that case, it would be very clear where liability lies, with whom, for making the decision of disclosure. In that case, the disclosure decision could be made by ICANN. If those conditions are not met, then we do not have that agreement, and the question is up in the air and needs further ironing. So that is my understanding and my recollection and conclusion from the conversation we had yesterday.

There is certainly a lot of bumps on this road. There is a lot of unknowns at the moment. There is also not a clear buy-in from the contracted parties side on this model. That needs to be further discussed within the contracted parties. All the conditions of ifs need to be ironed out probably sooner than later in order to see whether that path is viable or we need to look to any other option. So that is where we are on the fundamental issue of where the disclosure decision should be made.

Marika?

MARIKA KONINGS: Thanks, Janis. I think we had this as well as an action item on that. Staff is at least thinking of basically putting it up as a Google Doc, where each group can basically fill out what conditions would need to be met for the to accept either a situation where registrars would be then parties taking the decision or ICANN is taking the decision. That may at least give the group a good idea of what those conditions are and then allow for checking whether or not

those conditions can be met. I don't know if that's an action item that the group could deliver on in time for the next meeting.

JANIS KARKLINS: Yes. Stephanie first, Mar[k] following.

STEPHANIE PERRIN: Maybe it's the jet lag, but I can't remember the hypotheticals where it would be appropriate for ICANN to make the decision. My argument of course in ICANN and thusly reasoned to have an [independent] access point for this data is that ICANN has the authority over the registrars to de-accredit them. So it's a pretty crucial business/power relationship, and I find it inappropriate for ICANN to making those decisions.

So I'd just like to know what hypotheticals we brought forward as appropriate for ICANN to assume the controllership role there.

JANIS KARKLINS: Probably then my advice would be to go back and relisten to the conversation we had yesterday. I'm not claiming that my memory is perfect, but I still remember that the predominant opinion was that, in certain conditions, that could be the case. So those conditions need to be met. I advise everyone maybe to go and relisten to our yesterday's conversation for those who doubts on that.

But I will take everyone. Don't worry. Marc is first.

MARC ANDERSON: Thanks, Janis. Notwithstanding the fact that the Strawberry Team is hoping to talk to DPAs and getting additional responses on this topic, I think we heard pretty clearly on this topic from the Byrd & Byrd memos state that contracted parties are controllers for the purposes of disclosure and that contracted parties retain liability in the SSAD model.

So I think, from the Byrd & Byrd memo, we got our answer: the conditions were not met. So I think that's our answer. Unless we want to refute the Byrd & Byrd memo or we want to put everything on hold, waiting for a response from the Strawberry Team, then we have our answer and we can move forward with those assumptions.

JANIS KARKLINS: Thank you. No wait. The first is Alan. Alan? Or actually – Alan and then Ashley.

JANIS KARKLINS: Thank you. What I remember from yesterday was the decision. It's fine today to tell someone to go read the transcript, but I think we need to put it on paper real soon so we all know what we're talking about and not have this discussion again.

What I recall is Thomas' comment – I think it was Thomas' comment – saying it is only the party that makes the decision that could be fined and that it is conceivable but not necessarily obvious that, if it is a joint controller relationship, we could mutually assign the responsibility to make the decision on ICANN. That, of course, is all under the proviso that the data

commissioners are willing to accept that – i.e., the Strawberry Team – answer.

So, if all of those are aligned – the data commissioners accept it, ICANN has clearly assigned the responsibility, and the contracted parties have a high level of confidence that they have no liability because of the decision because of that (there's the issue of third-party liability also) – then those are the things that had to be aligned. That's what I call, which I think matches what you said. But I think we really do need to document this carefully.

JANIS KARKLINS: The process of how we have worked until now and will continue working with, because this is the only way how we can do that – after conversations, staff is capturing every idea that may gather or has gathered [on] mutual consensus or acceptance. Then that capturing is put forward to the team for confirmation. So this is how we got to draft zero, where staff was taking notes and then putting together a document that everyone felt is acceptable as a start for our meeting here. I think that we have fine-tuned a number of issues that we would need months to talk about during the telephone conversations.

Ashley?

ASHLEY HEINEMAN: I think it feels a little bit like Groundhog Day. Similar things happened when we met in L.A. last time, where we get to a point where we have this really delicate willingness to consider a path

forward, and then all the old fears come back up and we take a few steps back.

At least based on my recollection of yesterday, and perhaps a little of the day before then, is that, recognizing fully the liability concerns of the contracted parties and that they're real, there is a willingness to consider an approach outlined by Thomas Rickert that would – again, a lot of what Alan Greenberg said

But also, recognizing again what Alan said, ICANN needs to commit to this. They need to commit that they accept the liability risks associated with such a role and also get concurrence from the DPAs that this is something that they understand and recognize.

That being said, if it comes back and these things don't happen, we revert back to what we've been talking about, where the registrars play a larger role in the decision-making. But if the whole intention of a unified access model is to create efficiency and the predictability, I think it really behooves us to at least consider this as an approach. If that means also working in parallel, having something that makes the registrars feel more comfortable with a liability risk profile that has them involved, that's fine, too. But I think we're really missing an opportunity here to have the full benefits of a unified access model. Thanks.

JANIS KARKLINS: We're not missing for the minute anything. Only we're missing if we're stepping back seriously from what we discussed for hours the previous day. So that of course is a bit of a challenge.

I have further requests. It is Brian and then Margie and then Volker and James.

BRIAN KING: Thanks, Janis. I really am inspired by Ashley's perspective. I support going down that path and even working in parallel if we have to. But I think that we're in a place that nobody is freaking out and we can consider this option. We know there's a couple asterisks on a couple part of it, but I think we can collaboratively move forward in that direction. We have some other options on the table, too. I know not everybody loves my favorite one, but I'm ready to go in the direction of [inaudible].

JANIS KARKLINS: Nothing is ruled out at this moment, and nothing is agreed to at this moment. Everything will be agreed on when everything will be agreed on.

Margie?

MARGIE MILAM: Thank you. I'd like to also echo what Ashley said. Also, to Marc's point, remember that the Byrd & Byrd memo does talk about the concept of allocation of responsibilities. So I think that's what Ashley's proposal was based upon: this notion that, if we took this approach, ICAN would be allocated that responsibility and thereby, by doing that, there'd be a reduced risk. Everybody recognizes that there is a risk, so no one is debating that there is a risk. Ashley's approach is entirely consistent with the Byrd & Byrd

memo. So I know want to mention that's how I recall the conversation yesterday. Thank you.

JANIS KARKLINS: Also, I think that we are not expecting any answer soon from registrars and then registries, that they need really to digest and see what are those ifs that need to be put in place in order to go to that path. Those ifs still need to be worked out and agreed upon.

James was first, I was told, and then Volker.

JAMES BLADEL: Thanks. Just to address Stephanie's question – I think I'm in agreement with everyone as well – I think we decided there had to be a robust joint controller agreement that spells out these responsibilities and allocations. I think that we can agree on that conceptually.

But Stephanie put a point on this: what's the scenario where ICANN decides to release information as opposed to a registry or registrar? I just want to play that out for just one second please, which is there's only two scenarios. One, they had the data to respond, which means you guys would have a replica of all the data that could possibly be requested. Body language says maybe you don't want that.

UNIDENTIFIED SPEAKERS: [inaudible]

JAMES BLADEL: Right. Or Scenario 2, where a requester says, “Registry(registrar), give up this data,” we say no, and ICANN says, “We compel you somehow to give up this data, invoking our DPA-blessed joint controller agreement and therefore take the responsibility for …” You see where I’m going with this. There’s only two possible ways that this could play out. Either they had the data or they can force us to give the data. In both situations, they made the decision. They accept the responsibility.

So I think everybody is on board with the concept. I think our dream scenario is: “Take this all from us. Take all the liability. ICANN, you can have the data. You can answer the questions. You can deal with the data protection authorities.” Contracted parties will cheer and pop champagne over here and we can go home.

I think the problem is that we don’t know how to navigate between those things. So that’s what I recall. I also may have it a little bit backwards because I think we talked about this on Monday but we got the legal Byrd & Byrd response that articulated this on Tuesday. So we’re backwards a little bit.

JANIS KARKLINS: Volker is next and then there are a couple of reactions in the room.

VOLKER GREIMANN: Thank you. Taking the liability aside, I think some here are misremembering what Thomas said because there is a residual liability, not the 4% liability, which results from the data subject

making a claim against their contractual partner that may very well cause additional liability that we would not indemnified against, if I heard Goran correctly.

But more significantly, I have also have significant doubts on the ability of ICANN or any other third party to make a decision on the balancing test properly because they do not have the additional information that we have at our disposal that we can utilize to make that balancing test. They don't have the contractual relationship with the customer. They don't know which reseller the customer has made the registration to. They don't know who is the account holder.

All that additional information may inform our decision on the balancing test, and ICANN or any third party not having that information would reduce the quality of that balancing test. Therefore, it [inaudible] the liability of [inaudible].

JANIS KARKLINS: I have Chris, Ashley, and Alex in line, and then Alan. Chris, please go ahead.

CHRIS: James, I understand what you said and I appreciate it, but unless I misunderstood Alan, everything you said works but you would still be liable in the conversation that we had yesterday, Alan. If we're joint controllers and you're giving us stuff because we tell you to and then we're doing stuff with it, if we do that wrong you're still liable. Is that not what you said, Alan?

ALAN WOODS: Yeah. That racks my brain. Again, it really depends on safeguards. I do so many balancing—

CHRIS: You can build in safeguards and things to make sure that you're comfortable that—

ALAN WOODS: Yeah. If we're part of an SSAD and there is a requirement – we're joint controllers – for us that we are giving that data to ICANN in order to make those decisions on our behalf, we need to be satisfied that those decisions are being made correctly.

CHRIS: Right. So it's not that you would automatically be liable if we made a mistake. It's that you have to show that you – I might not be using exactly the right words – have satisfied yourself that what we were doing, generally speaking, was okay.

But in an individual case, you're not necessarily liable. You're liable if you haven't actually checked and tested that our processes, etc., are robust and to your satisfaction.

Is that fair?

ALAN WOODS: With the proviso that my brain is melting, yes. I think that is fair, yeah.

CHRIS: Okay. Thanks.

JANIS KARKLINS: Thank you. Ashley?

CHRIS: We're just talking. I'm not going to go away and write a document that says, "Alan Woods said it was fair."

JANIS KARKLINS: Ashley, please?

ASHLEY HEINEMAN: I think, again, there's a lot of hesitancy in this room, and I think for very valid reasons. But I think what I'm hearing here on this exchange alone is that it's worth detailing. It's worth understanding rather than making knee-jerk reactions that, no, it's impossible.

So I really encourage us to put it in writing. Let's test it out. Let's find the holes. If it doesn't work, it doesn't work. But I don't think we're in a position now just to say flat-out that this is impossible. I don't think that's fair to process.

I'm not saying James said that either, by the way.

Well, I hear a lot of knee-jerk reactions, and if I'm incorrect, fine. I'm sorry.

I think also I should put forward a third path. I CANN is going to hate me for this. I'm putting a lot of commitments on ICANN lately as potential ways forward.

UNIDENTIFIED MALE: Standing by to hate you.

ASHLEY HEINEMAN: Yeah. Great. It's that ICANN doesn't necessarily need to retain all the information. But if it's part of a contractual requirement that the information be transferred as part of this exchange and then, once it's (assuming) disclosed, it's destroyed (it's deleted, it's gone), isn't that another possibility? I see it still ties to what James' concerns were, but if you have it in the sense that you are contractually required to do so, you're then responsible for the transfer, not necessarily the disclosure.

Anyway, again, we don't have to make decisions. I'm just saying let's think through the possibilities. If it doesn't work, it doesn't work. But let's think it through.

JANIS KARKLINS: I think we did it yesterday. Actually, we did not discuss anything but the decision to disclose information. Let me add additional complexities that we have not discussed yet – probably at one point we also need to factor that in – and that is limitations of data

transfer to different jurisdictions. That comes to the point of data transfer.

So, for the moment, we are just discussing where potentially the decision of disclosure could be done and how the joint controllership that is suggested by Byrd & Byrd can be implemented and operationalized in a way that liability is fairly divided between two joint controllers. The liability kicks in for wrongdoing for that joint controller who makes the decision, not the other one. So there are ifs, ifs, and ifs that need to be still answered.

Alex?

ALEX DEACON: Hi. Thanks. We have may have moved past it a little bit, but let me just comment on something James said earlier. I think it's a follow-up to Ashley's last point, which is that I think, James, you mentioned that there is two models: one where ICANN discloses and makes the decision and owns all the data, and then the other one where, I guess, the registrars do that.

I think there is a third option, which is where ICANN is making the decisions but the data continues to live, distributed amongst the registrars, and they make queries as required based on the request.

So I – yeah. I may have misunderstand what you said.

JAMES BLADEL: I just want to be clear. If a request goes to ICANN for data, and ICANN gives that data, then ICANN has two choices. Either they have the data themselves or they can compel whoever has the data: registry or registrar. That was what I was trying to put it as. It wasn't really where it lived or where it didn't live. It was more that, in order for them to fulfill a request, either they had the data, or they know who did and had some leverage or authority to make them give it up. I was just trying to give the two paths there.

It's the second one I think that has me scratching my head because they clearly indicated they don't want all this data living on their – well, maybe not clearly. I don't think they want to – I don't want to do motivations again. But it's that second one I think we're getting twisted around on. How did they do that?

ALEX DEACON: Right. I agree. Thanks for clarifying. My point is that I think the data can still live distributed. There doesn't have to be one big, honking central repository of data at ICANN. It could still live distributed amongst the registrars, and it could be compelled – I think that's the word – when required.

JANIS KARKLINS: The devil is always in the details. But, again, if we look and listen to what Alan explained yesterday, to make a decision on even the balancing test you do not necessarily look in the private data of a data subject. You look to steps that the requester has done in order to evaluate whether that request is valid and whether you want, based on elements that are provided by the requester, to

disclose private data of the data subject. So I'm not sure, but I think that the private data comes into play in the process at the very end, not during the evaluation of the request itself.

UNIDENTIFIED SPEAKER: [inaudible]

Then maybe I misunderstood or was not overly attentive to description in Step 2.

UNIDENTIFIED SPEAKER: [inaudible]

JANIS KARKLINS: Okay. Then I'm taking back my argument. My apologies. I will stop intervening in substantive discussion because I don't understand much of it.

Alan G was the next.

ALAN GREENBERG: Thank you very much. In terms of compelling, ICANN already compels registrars to send data to thick registries. "We compel you to send data to escrow agents and things as part of the contracts." Is there a process by which you can refuse and not be sanctioned? I don't know. I think that's an edge case.

Volker's arguments about that, when making the final decisions, you have to look at the customer data is very persuasive. It's a strong argument why the decision should be left with the registrar.

On the other hand, having a uniform model that's predictable and handled in the same way for everything across all registrars is very attractive also.

Now, somewhere along the way, we're going to have to do that balancing test and decide which is the more important part. At this point, we're still trying to find viability of, is there anything on the other side to compare it to, or is there only one side? If there's only one side, we don't have to do a balancing test. That's the answer.

So, if we don't have the mechanisms of assigning a responsibility with appropriate liabilities to ICANN, then it's a done deal. But as long as we have that possibility, it's an attractive one, at least to some of us.

In terms of third-party liabilities, I think we generally agreed that, if ICANN is not willing to either indemnify you for third-party civil lawsuits or put together some sort of insurance fund or whatever, it's a no-brainer also. So there's lots of ifs that have to come together. Let's see how far we can do one path and, if necessary, work in parallel. Thank you.

JANIS KARKLINS: Thank you. Thomas?

THOMAS RICKERT: I think we haven't exhausted our imagination when it comes to dealing with this. I'd really like to encourage Stephanie to maybe do a little talk about the data trusting that you've suggested. I think none of us have really understand what you're up to. You've mentioned it a couple of times, but how this would work exactly I think is not clear to everybody.

I think that we are still revolving around a very limited number of choices and concepts. That doesn't do justice to the task at hand. You can think of multi-tier processes for this. For example, you could have a group of experts that say where the trust [is] that you mention. You mentioned that there should be a board consisting of representatives of the various stakeholders. It could be experts in international law. You could say that there are [inaudible] with these things [that] would or would not get access to the registration data in the first place. But they would look at the scenario and whether, in principle, the nature of the disclosure request coming from a certain jurisdiction with a certain motivation would allow for the disclosure of data.

Or you could give the data only to the data trust without permitting the data trust to pass it on. Leave the disclosure decision to the contracted parties but outsource the decision-making and the balancing test to the data trust, coming up with a suggested approach forward. That would not be a mere joint controller or controller/processor scenario. If they make their own determination, if they decide themselves by which methodology they're going to make the decision, that could be an independent controller, and you could find reasons for you to be able to pass on that data based on 61F.

So this is a lot of work, but let's not try to be in this box. I think we need to broaden this up. Also, if we can find an encryption expert, for example, let's talk about possibilities of encrypting data, of using mean of [synonymization] or partial [synonymization]. For these guys in particular, you might not need the real registrant data, but they might need to do different queries. I think we're scratching the surface. I'm sure that, once we get clarity on that, the other things will fall into their places because a lot of the anxieties will suddenly go away, I hope.

JANIS KARKLINS: Probably we need to further explore the options for this joint controllership and those elements of joint controllership. I even think maybe it would be useful if ICANN org and registries/registrars would find a way to sit together and talk through different elements of that joint custody, if you wish, and how that would work in reality so that at least those who need to sit in one boat would understand and would talk the same language. Just a thought.

I have Milton and then Stephanie and then Brian, in that order.

MILTON MUELLER: I agree with Thomas that we need to be a bit more imaginative about how we're structuring this. When we talk about centralization or ICANN versus registrar, there are certain things that can be broken down and centralized on one side while retaining decentralization on the other.

For example, I would be very much in favor of centralizing the request process via ICANN and having them establish uniform methods for requesting the different channels. But still they would effectively rely on the registrars to make the ultimate disclosure decision. If registrars were not really compliant with the overall policy, ICANN has sufficient leverage to monitor them and receive complaints about them and to sanction them as necessary.

So it seems odd to me that would think a centralized agency like ICANN would be fully capable of evaluating thousands of individual requests for data but not capable of supervising and monitoring the hundreds of registrars. It seems to me that ICANN is fundamentally in the business of accrediting, supervising, and regulating registrars. Even though they like to say they're not a regulator, that's what they do, fundamentally. I hope we don't get distracted by that. I just couldn't avoid using the word there.

So I think we could reconcile both interests in centralization and decentralization by looking at the request side differently from the response side from the different sides of the hamburger, if you will.

JANIS KARKLINS: Thank you. Stephanie and then Brian.

STEPHANIE PERRIN: Thank you. Looking way back, thank you, James, for returning to my question about those hypotheticals. I would suggest that a third hypothetical is that potential dog's breakfast of the request coming from law enforcement agencies in countries where there's

no MLAT. That's going to be difficult. If I were you, I'd outsource that one.

That brings me to this fundamental problem. I agree we were discussing this in the absence of the legal opinion, which lays out a lot of the fundamentals that we now understand better. We need to understand the double jeopardy situation that the registrars and registrars are in if they decide to delegate the decision-making on a disclosure of their clients' personal information to an organization that is less competent than themselves. By less competent, I don't mean that ICANN is incompetent. I mean they don't have the data, they don't have the relationship, and they don't have the local knowledge to make a proper decision about the rights of the individual in the context of that request.

So, by entering into a contractual arrangement of co-controllers with ICANN, one in which they are the weaker party in terms of the power relationship, they've made one mistake for which they are reliable. Then, if ICANN makes the mistake because of that lack of knowledge and releases the data or compels them to release it, that's Mistake #2: more reliability. That's what I mean by double jeopardy here. This is a no-win situation, as far as I can see. This is why we've been looking at the independent digital data trust: to create something that doesn't have these inherent conflicts to allow for deeper knowledge to bring in the kind of expertise that Thomas was mentioning because we haven't even talked about data flow here. But that's a biggie. I'm not talking about a central repository. I'm just talking about moving data [resonance] at the local level with the registrars to the requesters. Well, how? That's a big enough problem itself.

So that's all I'm trying to do: clarify these potentialities. But as I said yesterday, we are captured by this gestalt of a WHOIS database or its replacement. Then you start thinking that we're only talking about that data. The registrars are controllers of a vast amount of data, only the tip of which we're looking at here. But they must look at all the data they have in order to do that balancing decision. They would be incompetent if they did not. That is what's going to be examined by a data protection authority or, of course, in the event of a [inaudible]. Thank you.

JANIS KARKLINS: Thank you. I'm very compelled to know what is the relationship between the registrar and registrant. I do not have my domain name. I am not a registrant. My wife has one. All I know is, once a year, she frantically comes to me and says, "I got an e-mail, and I think it is spam because I need to renew my subscription for the domain name." So that's the relationship that I know between the registrant and the registrar. If there is something more than that, I would really like to understand just to have a full picture of services that registrars provide to individual registrants for their [services].

Now, Brian, you've been waiting long for a comment. Please.

BRIAN KING: Thanks, Janis. I sound like an Ashley cheerleader today, but I really like that suggestion. The thought that, if ICANN as the joint controller can due the data processing activity of disclosure after the registrar or the contracted party has shared perhaps the data

with their joint controller/co-controller, I think that has some real opportunities for us.

If we expand upon that concept, if ICANN is able to request and receive the data from registrars in the context that it's co-controller of the data, that addresses a lot of the things that I think we should be thinking later or in addition to the SSAD, like ICANN Compliance and how they can get data, how they can do ARS work. All kinds of things could happen.

So I think there's some real opportunities for that kind of concept. Don't poo-poo the concept if you don't want those things. I think that there's really some more that we can unpack from that. I'm looking forward to hearing more from Stephanie on the concept of this data trust, too. I think that might have some opportunities to separate in a real smart way the disclosing entity from the rest of this, if it makes sense to do that. So I'm open-minded and I'm encouraged that we're getting creative with how we can make this work. Thanks.

JANIS KARKLINS: Thank you. Chris is next.

CHRIS: Thank you. I wanted to build on what Thomas said and Stephanie. Whilst it certainly doesn't fit every nuance, and whilst there are bits of it that probably don't work, an awful lot of this work in respect to an independent structure has already been done. It was done in the Experts Working Group on WHOIS. The model that that group came up with – Stephanie, you and I spent two years of

our lives that we're not going to get back doing that, although probably we didn't call it a data trust. It was, in essence, an entirely separate body. There would be difference because of GDPR because we weren't looking at GDPR then. Fundamentally, if you want to go to that report and have a look, that does actually deal with some of the concepts and some of the challenges that you might face in this environment. And it may actually answer some of the questions on how it could be done. Thanks.

JANIS KARKLINS: Thank you. James?

JAMES BLADEL: Thanks. I forgot where we were going with this. I think it's this idea that we're still considering this. We're still talking about these conceptual things, but I just want to come back to a question. I'm sorry, Dan and Trang. You guys have been quiet. One of the scenarios is that you guys hold all the data and that you respond to these requests. Is that off the table from an ICANN perspective?

UNIDENTIFIED MALE: Yeah—

JAMES BLADEL: That ICANN has the data?

UNIDENTIFIED MALE: Nothing is off the table. We're quite because we have no real role in this.

JAMES BLADEL: Okay.

UNIDENTIFIED MALE: We're here to answer your implementation questions, except you guys decide what we do. There would be a lot of, obviously, risks and issues, and that would be a big decision that ultimately [inaudible] to the Board to take on that risk. We won't put them on the spot either. But we do your bidding. We're here to take your instructions, basically.

JAMES BLADEL: Okay. That's fair.

UNIDENTIFIED MALE: [inaudible] consensus on what to do, then the Board will evaluate that and then direct us to do it.

JAMES BLADEL: I thought maybe we could winnow this down a little bit, but that's fair. The second one is that, again, there's some authority where ICANN says, "We don't have the data. The registrar has the data. We're going to make the registrar cough up the data." Then the question I have – it goes back to a statement a made a couple days ago – is, if we say no and ICANN says yes, now we're in that

scenario where we discuss where we are now responsible for a decision that we didn't make.

Is that the double jeopardy that, Stephanie, you were alluding to? We could be sanctioned or say no to a data request that we didn't believe was legitimate but ICANN told us to. Under the joint controller that Alan was talking about, the allocation of liability (some of that) could still land on our doorsteps.

I think we established that that was a principle that everybody's head nodded on: people should not be liable for decisions that they didn't make.

UNIDENTIFIED MALE: If I could follow up on that, every time we should flip that around and say, are you [inaudible] ICANN org also should not be liable for decisions that you guys make?

JAMES BLADEL: Also agree. The decision and the liability are inseparable. If you are on the hook, you have to be able to make the call. If you're not on the hook, somebody is going to take that away from you. You can't get into a situation where I'm penalized for things that other parties are doing.

JANIS KARKLINS: Maybe that is a question that needs to be either asked or formulated by the Legal Committee and asked to Byrd & Byrd or by the Strawberry Team asked to the data protection agencies. In

the case … sorry? No, I'm just formulating a question and probably also a proposal. In the case of a joint controllership agreement and a clear distinction of responsibilities, how then does liability move? To explain. Please.

ALAN WOODS: That is one of the legal memos we received this week. We asked that question and we have our answer. We just need to digest that. We already have pushback. So let's look at that and –

UNIDENTIFIED FEMALE: And the Strawberry Team.

ALAN WOODS: Oh, and the Strawberry Team. Of course, yes. Thank you.

JANIS KARKLINS: Ashley, please, then Brian.

ASHLEY HEINEMAN: Oh, no. Not at all. I think what we're facing is we're just saying the same things over and over again. That's why I was recommending that we table this for now. We recognize we're going to consider it – that doesn't commit us to doing anything – and move on because I think we need time to digest because I think – at least I thought – I responded to a lot of what James just said, but I think we would need time to think about it. Anyway, I'll leave it at that.

JANIS KARKLINS: Brian, please?

BRIAN KING: Thanks, Janis. I'm happy to move on, too. I would like for us to think about – not answer now so we can move on – whether we would like to ask the Board, who's ultimately going to make the decision about this, what their answer will be in such a context. I don't know if a lot of us love the idea that org would have a big mass of all the data, not in that context but in the context of joint controller, where James is talking about how the party who's doing the disclosure is on the hook. If that's passed here and by Council and goes to the Board, what's the answer going to be? We should know that now before we go down that road. Thanks.

UNIDENTIFIED FEMALE: Isn't it also true that the contracted parties mention that ICANN org and the contracted parties are discussing the content of a joint controller relationships, too, which might help inform what does go to the Board and feed into the Strawberry Team input in all of that piece?

JANIS KARKLINS: Chris?

CHRIS: If you want to write a letter to us that says, "One of the things we're thinking about is X. Several of the things we're thinking

about X and Y. And what that would mean is Z. Is there anything you can tell us that would help us to whether we're going to end up wasting our time if we do down that road?" I think we would work hard to try and respond to that letter in a timely way and in a way that was helpful, rather than just saying, "Thank you very much. Indeed, interesting concepts. We'll let you know."

I've got no clue what the answer would be. I've got not clue how we would get to the answer. But I think you're not going to get an answer unless you try. I recommend that you think about putting something in writing to us and [inaudible].

JANIS KARKLINS: I think, with that proposal, we conclude this part of how far we have gotten. I though that we have gotten slightly further than we are now, but that of course is part of life. We will first revisit the question.

Coming further than where we are, I acknowledge that, on the supply side, there are a number of building blocks that we have not touched yet or touched briefly. These building blocks, though they were not recognized as of extreme importance for the face-to-face meeting, need further reflection and anything. Hence, all these things we would continue working on.

In my mind, we can easily continue working on all building blocks, which would then become part of the standards. I'm not saying "system" intentionally but standards because, with whatever system we will agree on, standardized building blocks will

complement that system either without modification or with minor modification.

As a result, my proposal would be that we continue working on our regular meetings on Thursdays, starting with a meeting tomorrow, on those … I'm just checking for whether they're listening.

UNIDENTIFIED FEMALE: [inaudible]

JANIS KARKLINS: Starting with a meeting a week after tomorrow, we continue to plow through and then try to establish the base for an initial report. I think we have about eight or nine meetings between now and Montreal. We need to strive to accomplish as much as we can. I think that we can use the same method as we used before to take a building block to one reading in one meeting and then ask for further input and then try to preliminarily close the conversation on that particular building block in a subsequent meeting. Then we get to Montreal with a document that we could then review in Montreal and see whether we could progress any further on a systemic discussion. So that is essentially my proposal leading towards the Montreal meeting.

Milton?

MILTON MUELLER: Just a question on the procedure that you proposed. I think one of the key issues we're stuck on or need to resolve is the question of

decision-making regarding disclosure. I'm not seeing how that maps to a particular building block. Can you map it to one of those, or does it not really fit?

JANIS KARKLINS: I think we need more information about it. You heard a proposal that Chris made to the contracted parties to formulate questions in relation to the joint controllership and how that relationship operationalized and how the—

MILTON MUELLER: Do you think we have time to do that?

JANIS KARKLINS: Sorry?

MILTON MUELLER: Do you think we have time to send them a letter and get the response before Montreal?

JANIS KARKLINS: Again, that is a question not to me. It's a question to the contracted parties: how long would—

MILTON MUELLER: Do you think we have time for that?

MATTHEW CROSSMAN: Sorry. I didn't think, Chris, that you were suggesting that came from contracted parties. I thought that was for the entire group to formulate a letter to send.

CHRIS: [inaudible]. Frankly, I don't mind where it comes from. I think the key question—

UNIDENTIFIED SPEAKERS: [inaudible]

CHRIS: I really don't. One of you can write a note. I don't care. What I think what you want, if I've understood you correctly, is to understand whether or not we think something is a red flag. If we think it's a red flag, then we would tell you.

Now, what I would strive against is us coming back to you and saying we can't possibly answer that question until we have more information. I'll not say I'll succeed in striving against that, but I am saying that, I think, if you asked us a question, our job is to say, "Is that a red flag?" So ask the question, or –

UNIDENTIFIED MALE: But don't you provide the first version of the draft?

CHRIS: So you're going to need to – yeah, you can do that as well, I think.

JANIS KARKLINS: That certainly is an issue that we need to discuss: whether we would be able to discuss until Montreal or at the Montreal meeting. That remains to be seen. But we will not escape that conversation, for sure. But we have plenty of other things to do in order to progress to an initial report.

I also see that, as a result of this meeting, staff will produce and table a 1.0 version of the draft. For that probably we would use the same methods. We would put that on the wiki, where everyone can provide comments/inputs to the document going forward.

So my aim would be, in Montreal, if possible, to come with a document that could demonstrate substantive progress in our advancement in our work, even if there might be some unanswered questions, and then, After the Montreal meeting, assess when we would be able to table the initial report.

Stephanie was first – Alan was waiting a long time, then Stephanie, then Chris.

ALAN GREENBERG: Thank you. In support of your proposal moving forward over the next few weeks, Milton earlier said that he could support a single entry point managed by ICANN that then gets fed down to the decision makers of the contracted parties. A lot of the blocks that we're talking about apply even in that simple model, especially if the centralized system does some triage or assessment, not the decision but preparation for the decision – the kind of things that Alan was talking about yesterday.

So I think the way going forward has merit regardless of how we do it because, if we only end up with a centralized place to make the request and logs the request and keeps the records and then funnels it out, we're a lot farther ahead than we are today.

In terms of how we actually come to closure on what we do, we have been thinking here of all black and all white. I think any reasonable solution is likely to be a zebra. That is, some parts are white and some parts are black. We may well find a whole class of requests where the kind of request and who it comes from are things that we end up feeling comfortable making automated decisions on. It may not be the majority of them, but it may be a significant bulk of those. Those could be [inaudible] automatically. The rest just get fed down. The registrar has the benefit of all their customer data and making those decisions.

So I think we need to stop thinking of A or B because I can't see any solution where every single case is handled with a single way. Thank you.

JANIS KARKLINS: Thank you. Stephanie, please?

STEPHANIE PERRIN: I'm going to say it again. I've said it in every working group I've been in. Sometimes I feel so lonely because I'm the only one apparently that has actually done this job of figuring out privacy procedures. People don't intuitively think this way, apparently. We don't need to do anything. We're in an EPDP. It's a policy development process. We develop the policy. Underneath the

policy are the procedures. We control the entry point right now by writing procedures. It's already there under all the existing contracts. So this is not rocket science. We should know that we are going to be doing this and that ICANN has a responsibility to do that. That's their role. What they don't have a responsibility to do is make a decision. That is totally separate and different.

I know I sound really petulant at this point. It's been a long three days. I'm discouraged that we don't seem to have some of these kind of fundamental concepts that those of us who've worked in data protection down pat by now. So, yes, it's easy enough for us to develop the procedures as we sort them all out. We need to thinking of that now as we go through the policy.

What the heck did I raise my hand for? Yes. Back to the next draft of the report, Marika had raised the issue of should we be looking at legal basis instead of some of these other issues. [We all went, "What was] the decision on that?" because I think that's a great way of helping us get further along in this discussion. And, if so, would it be useful in terms of raising questions because I heard an invitation to raise questions. I've got lots. I'd like to sort them in a way that is most useful. To me, the most useful way would be, under these legal grounds, what questions arise, based now on the new legal opinions that we've received? So that was why I raised my flag. Thanks.

JANIS KARKLINS: I think that everyone can raise everything. Then there is a standing invitation to each team member to provide input to any unresolved questions that we have: building blocks or any other

issues. So I would be very happy to see that team members volunteer to do the initial write-up that would help us to talk through and develop policy recommendations. That is our ultimate goal.

If Marika wants to ask a question, or—

MARIKA KONINGS: Answer.

JANIS KARKLINS: Answer, yeah. To provide an answer.

MARIKA KONINGS: Just to try to answer the question, at least where I think staff is thinking at the moment is indeed to develop a kind of table that would outline the different lawful bases and then map on a horizontal some of the other aspects: what does the request need to provide, what is the expected timeframe for a decision, is automation likely? Again, some of those answers are already, of course, in the zero draft. I think what we're trying to establish is should there be differentiation depending which lawful basis is applied.

I think Thomas gave me the idea as well that, maybe as part of that, we also add a column and say what are some of the standardized scenarios or categories that are likely to fall within that lawful basis which could potentially be used for the development of a template for a standardized response.

So I think that's where at least staff's thinking is at. Of course, a lot of that aligns closely with the building blocks and it may require then further spelling out in some of the building blocks if there is indeed differentiation. But I guess the expectation is as well that in certain cases it will be the same: maybe some of the information that needs to be provided or some of the elements. That's at least what we took away. Our thinking, our homework, is after this meeting.

JANIS KARKLINS: Thank you. Chris?

CHRIS: Thank you. Two things. One, I just want to clarify what I said about asking us the question because I said, I think, I don't care if just one of you writes a note, at which point Dan nearly passed out. Obviously we need to get a question from the group that says, "We're thinking about this. Can you please …" etc. Individual questions from each member of this thing isn't going to fly. So hopefully that's caused down Dan a bit. Everything is okay.

Secondly is if I could encourage Alan Greenberg not to refer to this as a zebra because all that's going to do is encourage Goran to move on to animal names for a project. We really don't need to do that. Thank you.

JANIS KARKLINS: Maybe I can ask the contracted parties to do the first write-up of the questions that you think need to be answered for the quick

look by others because, ultimately, that is basically a marriage contract, if you wish. That is your marriage, not others'.

UNIDENTIFIED SPEAKERS: [inaudible]

JANIS KARKLINS: Then we will look. It's entirely in your hands when you will be able to present that list of questions. So we will look at it immediately once we receive it for further transfer to ICANN org.

That should bring us to Montreal. In Montreal, we will have one full day on Saturday and then one slot of – oh, yeah. Okay. If, Marika, you could tell what awaits us in Montreal.

MARIKA KONINGS: Thanks, Janis. We'll also circulate that on the list. On Saturday we've currently carved out a meeting time from 8:30 to 6:30 in the evening. On Sunday, there's a slot from 5:00 to 6:30. I think we've currently labeled that as a potential prep session for the plenary session that's scheduled on Monday.

I think there's still some discussions going on between, I think, the GNSO and the GAC on how that session should look like. I guess there's an assumption or an expectation that it would involve the participation of the group. So we have the potential to use that slot for that.

There are also some slots on Monday, but I think we're still waiting on a final confirmation on whether the opening ceremony takes

place in the morning or in the afternoon. I think it's dependent on the availability of government officials in Canada. I think, for now, it looks like that will be in the afternoon, so we have a slot from 8:30 to 10:15, which would be followed then by, from 10:30 to 12:00, the plenary session. That's the previous cross-community high-interest topic sessions, for those that may not be familiar with it.

Then we have a wrap-up session from Thursday from 1:30 to 3:00. I think we also have the potential of having, on Monday afternoon, a slot before the opening ceremony. But I think we probably need to see if three slots in a day may be too much. But I think that's currently reserved as well. We'll share this list as well with the group.

JANIS KARKLINS: I don't think that we have too much time. I think we have too little time to conclude our work. But that's the plan for Montreal. If we will have sufficient progress, then the idea would be, if ever possible, to publish the initial report in early December – in other words, four weeks after Montreal. If that will not be possible, then we would continue our online work, and we would meet face-to-face the last week of January, again, for three days, as now and then for sure finalize the initial report. The dates that have been penciled in in the calendar is 27th to the 29th of January.

[ALAN WOODS]: Thanks again for my birthday. Wonderful.

JANIS KARKLINS: We expect that you will bring champagne with you then.

[ALAN WOODS]: Yeah, absolutely. Correct.

JANIS KARKLINS: But if we will manage to produce the initial report by the end of December, then the January meeting will take place anyway because then we will review comments for the initial report and we'll start working on the final report. So that is the plan going to Montreal, beyond Montreal, and heading to the March meeting of ICANN.

Stephanie, please?

STEPHANIE PERRIN: Thanks. I would just like to put on the table that this report is too important to be looking for comments over the Christmas period. We've done that kind of thing before. We don't get the kind of comments we need. It reduces the credibility of the final product if we do that. Thanks.

JANIS KARKLINS: Brian?

BRIAN KING: Thanks, Janis. I do regret that it would be over the Christmas holiday. I guess there's two alternatives. One is to get it out faster,

which I think, if it were possible, we would do it. The other one is wait until after the holidays. I don't think that's a good idea. Thanks.

GREG: Very quickly, the public comment period must be a minimum number of days but it can also be longer than that. You can release the report before the holidays but also build in a week or two weeks of extra time because you have holiday breaks. So that just determines your end date. Thanks.

JANIS KARKLINS: I'm optimistic by default. That's why I am saying "if ever possible to release the report." Looking at the stage where we are, it will be a miracle if we will pull up and introduce a report by after the Montreal meeting. Then, of course, we still have outstanding issues and Priority 2 issues. If we will not manage to get an initial report done by early December, then most likely we would logically need to bring Priority 2 issues in a conversation before the January meeting, hoping that we could also outline the proposed solutions for Priority 2 issues in the initial report because, in early December, if we manage to get the initial report for early December, then of course they would not contain Priority 2 issues at all. I would not even attempt to bring Priority 2 issues for conversation prior to early December. So that's the plan.

In order to get to the final report, we will need to really rely on our wisdom and also flexibility because we can agree only if we want to agree. If we [camp] on our positions and do no listen to each

other and do not try to bend our longstanding positions, then of course it will be difficult to agree. So, again, my call is not to give up and just keep working.

With this, I would like now to open the floor and see whether there is some kind of violent disagreement with the proposed way forward.

Ashley, please?

ASHLEY HEINEMAN: Not violent disagreement. For a sake of a little bit of perspective, where does that mesh up with what we articulated as our planned timeline? Are we generally in the same path? It sounds like we're taking a bit longer than we anticipated. I just want to get a better understanding of where we are. Thanks.

JANIS KARKLINS: From the initial thinking, we're still in the range. We will not be in the range if, by the end of January face-to-face meeting, we will not be able to finalize the initial report. So, if by the end of January the initial report will not be finalized, then we will be out of range. Then we will be in trouble because [Barry] is asking for the floor.

[BARRY]: I think, to be more precise, our critical path is early December for an initial report. If we miss that date – and with the holidays – then that pushes us out by two months.

JANIS KARKLINS: Matt?

MATT SERLIN: Thanks. Not violent disagreement. I would just caution us all against getting into the frenetic pace with which we closed out Phase 1, even with the initial report. I think, for those votes who are participating on the IRT, there have already been some things that we missed in the final report in Phase 1, so I would just make sure we're all mindful of that and we're not – James, you have a phrase for sacrificing quality for time, right? Is that your—

JAMES BLADEL: [inaudible]

MATT SERLIN: Oh, I got it right. Thanks.

JANIS KARKLINS: Somebody in the group yesterday or the day before yesterday said that, from experience – that was a long-timer in ICANN – the quality of the report is inversely proportional to the time the PDPs have taken or had taken to write those reports. As a result, also there we need to strike a balance. We need not to rush, but we also need not to kick the can down the road because we will not be wiser tomorrow. If we can make a decision today, then we need to make a decision today. Tomorrow will not be different. So, of course, there is circumstances – we heard some dependencies

that we need to factor in in our schedule – but ultimately it is our collective responsibility to agree as soon as we can.

Please, Greg.

GREG AARON: A question to help us keep on schedule. The Legal Sub-Team, I think, has some additional questions it's looking at. So, of course, we want to get them out to Byrd & Byrd so we can discuss them. In next week's meeting, can we get an update from the legal team?

JANIS KARKLINS: Yeah, for sure. Caitlin, when is the legal team meeting next?

CAITLIN TUBERGEN: I think the legal team isn't scheduled to meet next week but the following week. But perhaps – well, Leon is not in here – the legal team can reconsider meeting, just coming Tuesday to talk about some of the issues coming out of the face-to-face.

JANIS KARKLINS: Yes, please?

UNIDENTIFIED MALE: I think the legal team is scheduled to meet this Tuesday, unless something has changed in the interim.

JANIS KARKLINS: No, nothing has changed.

UNIDENTIFIED MALE: Okay.

JANIS KARKLINS: So, good. We will have updates of the legal team. We are – Alan?

ALAN GREENBERG: Quick question. When will we see the agenda for Thursday?

JANIS KARKLINS: As usual, on Monday. I think we're at the end of the conversation that I was planning for today, but lunch hasn't arrived yet. I heard some interest from team members and also myself on the concept that Stephanie suggested on this data trust. Maybe we can use the time and do a five- or ten-minute break and then reconvene.

Then, Stephanie, if you could outline your ideas and how that trust could work and how that could fit probably in the SSAD project if we can agree on SSAD in whatever shape. Would that be acceptable to you? I thought yes because yesterday you said you would be ready to speak on that at any time of the day. So let me know.

A break for ten minutes. Please come back to listen to Stephanie on the data trust concept.

[inaudible] that we can listen to the outline of the privacy board that Stephanie had mentioned on a number of occasions. Then, of course, any questions you may wish to ask to Stephanie that will be possible as a result.

Stephanie, all attention is to you.

STEPHANIE PERRIN: Thanks very much. Obviously, this is an impromptu discussion, so I don't have a PowerPoint or any of the other things that one is supposed to have. However, basically what this project was and is it started last year. We put in – we being me and my doctoral dissertation advisor at the University of Toronto, Andrew Clement – a proposal to the Office of the Privacy Commissioner of Canada under their grants and contributions program to look at disclosure of WHOIS data and whether the development of standards – preferably international standards – would bring greater confidence in that disclosure process.

Those of us who survived the RDS battles – I'm looking at Marika here – know that we had quite a bit of discussion with cyber security research about how the end of the world was at hand, unless they continued to get this. The fundamental problem is, how do you ensure trust in the recipients of data who put forward a claim that they need it for purposes that are … Definitely the purposes of legitimate, but are the actors legitimate, and are they fulfilling those purposes?

We don't have that problem with law enforcement because, in a data protection regime, when you give data to law enforcement,

they certify who they are, what their name, rank, and serial number is, what they're investigating, and what article code of the criminal code that they're acting under. You give them the data and you know that they are a public body and they have oversight and you're done and dusted. That's why we like MLAT, too. Same reason. Somebody is certifying that it's going to who you want/ However, there are a number of other valid actors that need data for their purposes.

So we've put in the bid. We were, as I say, focused on cybercrime because it was relevant in the Canadian context. We had a workshop in Barcelona. We discussed the potential standards. [Mark Svancarek] was there talking about the Microsoft approach to standards and abuse. We had Richard Wilhelm from Verisign talking about the RDAP standard and what it did. We had SSAC folks. We had Rod Rasmussen, and Greg came, I think. Did he? No. It was Patrick.

Basically, at the end of the day, the civil liberties folks that we had invited to the workshop – all of this is up on the Barcelona site, plus on the privacystandards.ca (the recording of the event and the presentations that were given at the time) … The proposal coming from the Canadian Civil Society folks – that would be [Civic] from the University of Ottawa and the Canadian Civil Liberties Association, who do quite a bit of litigation in this area on fundamental rights – was, "Why don't you look at a data trust?" because fundamentally the problem is not so much the management standards of the actors that are requesting the data but the trust relationships in that transfer chain of the data.

So we took that on board. We had a look. We hired a researcher who'd been doing independent research for the Sidewalk Labs project in Toronto that is being basically run by Google's Alphabet division. She complied a bibliography of current work on data trust. It's a new concept. There's very little scholarship on it. We have that bibliography also up on the website for those who are interested, and we have a brief summary report of the conclusions reached.

Now, we went forward and applied again. The applications for this are up on the Office of the Privacy Commissioner of Canada's website. They gave us another grant this year to study data trust as a concept in several applications. So my colleagues are working on the Google Alphabet project and how you would share data in basically a surveillance site, to put it bluntly. There's a lot of data. There's facial recognition. There's transit capacity. There's you name it. There's all kinds of data being gathered. Everybody is participating, including our various levels of government, all three (municipal, provincial, and federal). They all want access to that data, and so do the vendors, and so the apartment developers.

How do you decide what's fair in that kind of a context? Well, the data trust that is not being managed by one of the governments or one of the vendors might be a good method.

So it's early days on that project. We got the grant in April, and we complete next March. I will be looking at the development of the ICANN model focused on the TSG report and some of the policy issues that are not drawn out of the policy assumptions, that are not drawn out in the TSG report. My colleagues and I hope to

come up with a framework for assessment for what you need in a good data trust.

Now, fundamental concepts in a data trust. Just of the top of my head, we would look at a board structure. This is an international governance system in a global information society. So you need regional representation. You need different types of policy representation. You need representation of the actors that are putting in the money and the goods, and the stakeholders, as we would say in the ICANN context. We need to find the trust points where we need to build in some independence.

So, as Thomas suggested earlier, we would have international legal experts looking at the data flows. For instance, there's been quite a bit of discussion back and forth on consumer protection. Consumer protection is a valid reason to disclose data. But how do I know, if I'm a registrar, if that person is legitimately looking for consumer protection and isn't a crook or an ex-spouse looking to get an address to kill somebody? So it's those kinds of particular types of expertise that are group-related, that are the kinds of stakeholders that we identified here. Depending on the volume, we need to bring those people in.

One of the concepts that I have in my head – it might be a false gestalt … I think of CRTC, our Canadian Radio and Telecommunications Commission, that has regional representation and different expertise on the different types of communications: broadcast and satellite and telecom and all the rest of it – Internet, ISP, and consumers. They're all represented there.

So that's the concept. Of course, it's even more complex in the ICANN environment because it's got to be global. You got to have different countries represented. You have to represent different legal traditions. So putting that all together and figuring out how to do it is not a simple task but one that maybe we could think about because the number of applications of this is really growing. We're hoping for another more expansive bibliography this year. In a global information society, these things are cropping up all over the place.

Of some of the models that already exist that work or do not work that we may be looking at, clearly the oldest would be the credit reporting system that we have in North America, which may not be familiar to some other countries. The Equifaxes and the Transunions of the world have been the trusted holder of all kinds of credit information. They may or may not have access to government Social Security information that keep that accurate. Their accurate rate is about 60% consistently, last time they checked. The privacy advocates have been hammering away on the doors of that for decades and getting nowhere. So it would be, I would say, even though it functions very well, a failed model from a privacy perspective and a reliability perspective. But that's my personal view.

But there are other models. With the fish tank models for spam, we had the same kind of problem: who do we trust to run this kind of thing, who's got access to the data, and what are they doing with it? A trusted model, of course, would be the financial crimes reporting center. Even in Canada, we have put those guys under a triennial cyclical audit of the privacy commissioner. That's a

trusted government system. There are other models: medical information (the Canadian Institute for Health Information). That's really a good model of a data trust because it is independent and has a lot of procedures and fee schedules and audit to ensure that the recipients of personal health data have [identified] it at the appropriate point and that the data has only flowed in a controlled way.

So I think that gives you an [inaudible] of what we're doing. We were thinking of having a workshop in Montreal. But yours truly was supposed to organize it so I don't think it's going to happen. Maybe. I do have a commitment. I think I mentioned that my colleague, Lisa Austin, of the University of Toronto law department, who is one of our constitutional scholars for privacy in Canada, has another project going – well, two really – one with Ian Goldberg, who is a colleague at Waterloo, on anonymous legal queries for law enforcement (anonymous and untraceable). I've talked to him and Roger Dingledine of Tor about how to do this for our model. So we have an anonymous database query system that we hope to integrate. She's also working with banking fiduciary trust scholars on how the financial trusts work and what concepts we can bring over from the idea of a fiduciary/financial trust to this. Nobody has done that kind of work on the data side.

So is that enough to get started?

JANIS KARKLINS: Thank you. Where do you see this idea of data trust being placed in the SSAD model? If you could elaborate a little bit. But let me give also Alan and Greg and Brian afterwards a chance to speak.

Alan, go ahead.

ALAN GREENBERG: It sounds fascinating, but I'm not at all clear how that fits into the model we've been talking about, not of the SSAD but of controllers and liability and where the data is held. I'm not quite sure how this solves our problem.

JANIS KARKLINS: Greg?

STEPHANIE PERRIN: Uh—

JANIS KARKLINS: Let's collect a few comments and then you can answer. Greg, please?

GREG AARON: Thanks for the explanation. I don't understand what it could do for us. I'd like a more concise description of what role it fulfills. For example, will it help us figure out how to accredit people? What exactly would it do? Thanks.

JANIS KARKLINS: Brian?

BRIAN KING: Thanks, Janis. I had the advantage of having discussed this with Stephanie yesterday, so I can give some thoughts on that. I wouldn't pitch this as a cure-all for everything that we need to do, but one thing that I think is interesting is the concept of the fiduciary duty between the trustee and the beneficiary of the trust. The data is placed into trust. That can have some interesting utility for us as far as incentives in the system and the fact that some folks that might be processing the data have an interest in how that works. In a trust context, fiduciary duty would be from the trustee or the body that's acting as that to the intended beneficiary. So you have to be clear about who the beneficiary should be.

The way that I would, if we intend to consider such a thing further, imagine that it works, to Alan's point, could be that we would develop all the parameters and everything. We're going to do everything that we're doing here anyway, but rather than perhaps asking ICANN to be the party that makes the decision about processing the data, some other party – the trustee in a trust context – is given the same parameters/the policy principles we've developed from the SSAD and instructed with instructions that they can't ignore to operate in this fashion. That's how trust works: the trustee is given instructions – "Here's how the funds or the data can be distributed and under what terms" and things like that" – and then the trustee has to act in the manner that their given in how the trust was established.

So that's the way that I would see it working: the policy principles would be handed to the trust, and the fiduciary duty relationship takes over where we have some questions about the incentives of

whoever else might be disclosing the data. So it's interesting food for thought in my opinion.

JANIS KARKLINS: One of the arguments was the competency. "Well, ICANN cannot do it because it does not have sufficient competency in making decisions on disclosure [and] trust where the competency would come from."

Stephanie?

STEPHANIE PERRIN: How this would work … Basically, the concept for me of ICANN doing this has too many conflicts. There's too many unequal power relationships. ICANN frankly doesn't have a good history in terms of looking after the interests of the registrants. If you look through all of ICANN's procedures and policies and protection measures, protection of registrant rights is not high on the list. We had a procedure for a charter registrant's rights and responsibilities, and the word "rights" was removed.

The fundamental mission is to act in the interest of the registrant here in terms of protection of their data, recognizing all of the valid interests in law enforcement and trademark protection and all of the other issues that need to be dealt with. But, if it were trusted by the registrar and if it were controlled in such a way that the potential for liability would be decreased, then it would be potentially more affordable as an option to ensure and to take the liability aware from the contracted parties.

Right now, I would not blame them if they did not believe that they could be absolved of liability. If you were to give much of your data request functioning to an independent autonomous think tank, basically. It's not going to have the data. It's going to have control of the requests. It will be that funnel, to answer Greg's question about accreditation. All of the parties that need to accredit their actors will have to come to this think tank and say, "Here's our accreditation procedure. This is who we're accepting as a cybercrime researcher, a trademark lawyer, a (whatever), a law enforcement official." Potentially it could streamline the MLAT process, although it's up to registrars whether they want to handle that one themselves.

There's still going to be, because the data is going to stay with the registrars – the SSAC were adamant about that, Patrick in particular. You don't move the data any more than you have to, but you don't need to. I learned that way back in the EWG. A distributed model leaves the data with the controllers. You're still controllers because you have the relationship with the client, but you have a trusted entity that is going, at the human intervention point, "I need some data to evaluate this request. Tell me how to respond." That's not abnormal. That is the way requests are handled in the existing world where we get these things. Hospitals, for instance, go through that all the time over medical records requests. So this is not reinventing the wheel here.

JANIS KARKLINS: Ashley, please?

ASHLEY HEINEMAN: I'll try not to be long-winded. I have a lot of stuff. This is interesting. I'll try to keep it intelligible [inaudible]. I think this is interesting and I don't want to sound like any of my comments in any way—

STEPHANIE PERRIN: No, no. Go for it. I'm not sensitive about this. Go ahead.

ASHLEY HEINEMAN: It's interesting and I like it only because [inaudible] something not totally similar, but in the DNESSEC space, with the trusted community representatives, it added a lot more complexity but it added a level of trust to situation. So I see the value in that, but I'm also a huge advocate for getting this done quickly as well. When you add complexity to something, you typically add more time to it as well.

I'd also be interested in maybe furthering the conversation because it's not clear to me that what's actually being proposed actually addresses a number of the concerns that you've raised in this conversation, which is the need to be close to the data and the view that ICANN – this is putting words in that weren't words that you used but it's how I interpret it, so I apologize in advance – can't always be trusted.

But what I see is that, at least from my perspective, ICANN is in a position to be trusted because they have a greater level of accountability. I'm going to see [it's in] the contracted parties, but not because I don't think you aren't trustworthy but only because I think there is so much rigor in ICANN when it comes to

accountability. You have the stakeholders – I would think you would agree with me, Milton, to a certain extent, considering you're part of the accountability process with the transition. It's not necessary completely applicable in this case, but maybe that's something we can consider: making it applicable to this. The fact that you have the variety of stakeholders watching ICANN and doing this – again, I'm not wedded to ICANN being the decision maker. Just throwing that out as a counterbalance to what we're talking about.

All that being said, I think this is interesting, and I'm certainly happy to continue having the conversation.

JANIS KARKLINS: Thank you. Greg?

GREG AARON: Hi. Does this group have an operation role in any way? Let me explain what I mean by that. One of the things we have to figure out is how do we accredit people and set standards for that. It sounds like this group would be involved with that. Is that right?

Okay. Another thing somebody might have to do is define use cases where we might be able to find commonalities and maybe even automate certain kinds of things. So somebody has to figure out what those are. Does this group potentially have a role in that? Does this group give thumbs up or thumbs down or actually get involved in individual decisions? The people who've made requests for data – are they now looking at these? Or are they up above, more at a general level?

STEPHANIE PERRIN: Obviously I haven't written my draft report for how this could work so far for this year. I'm going to propose several models, probably three. That's my favorite number for models. Any more than that and it gets too complex.

I take up Ashley's point. There's added complexity here, but if it leads to more trust, it's probably a good thing because trust is one of our problems in this whole discussion. We could do all this work, and if nobody trusts it, it's not going to work.

The other thing that this simplifies is embedding different actors for different types of requests. I am a firm believer that that, particularly in the balancing test question – if the registrars want to elect one of their members to go in there (let's take Ben) and be the trusted actor that does the balancing test on these things, they are sure that their balancing test is being properly applied on that. The other entities at the table at the board there accept him as an actor who has expertise in a particular area. This can be rotational, so you can manage a multi-stakeholder model here.

[GREG AARON]: Let me ask this. My concern is operational efficiency. If requests come in from data requesters and then there is a committee or someone designated by a committee that looks at all of them, that would be unbearable load.

STEPHANIE PERRIN: Yeah.

[GREG AARON]: And slow, too. So, if that's not the model, then you've answered the question.

STEPHANIE PERRIN: Right. That's not the model. The model is like a sluice/gate through which the requests flow. They go to the registrars. If all the template requirements are met, the data comes out again. If a balancing test is required just to tick off a bulk – in your case, really a lot of thinking has gone into how we make sure we get the cybercrime stuff dished out the same day without doing a sloppy job here. So you've got a guy in there watching this and approving a bulk request – Milton may shoot me for this – as long as all those templated requirements are met. Same thing for anonymous law enforcement requests. If [inaudible]—

[GREG AARON]: That what strikes me as an everyday, 24/7, day-in-day-out job.

STEPHANIE PERRIN: Yeah. It's a full-time job. And it should be a full-time job. If nobody is watching it right now, then I'm worried.

[GREG AARON]: I'm going to [inaudible]. Yeah. That's a big job. I don't know anything about this program because Rod and Patrick did not bring anything back to SSAC when they were—

STEPHANIE PERRIN: I'm crushed that they didn't come back and talk to you guys.

[GREG AARON]: They were not there in an official capacity. So lots more learning to be done.

STEPHANIE PERRIN: Yeah. It may be a whole team that has to do it. But it improves the trust level, it's good.

JANIS KARKLINS: Alan, your [inaudible] was up before Georgios'.

ALAN GREENBERG: Just one very brief comment. It sounds like, if we're now moving this decision process into the trust, we are transferring responsibility from the registrars into the trust. I start asking the question of who's going to fund this trust.

JANIS KARKLINS: Georgios?

GEORGIOS TSELENTIS: Thank you, Stephanie, for bringing this to us. When you started, I was trying to figure out, when you were saying "trust," to which part you were referring to. It was trust not to reveal personal

information? For us to reveal relevant information to requesters? Or to reveal to adequate requesters? So these are different things.

But you gave an example that these trusts exist in the medical, you said, sector and in the trusted holders of credit info. This rings a bell from previous experience, where you have a lot of personal data in this later case, where people want to – this is also related to SSAC – process the information but this information can be anonymized. Make a feature selection about exactly what you want to do. For example, with the credit example, you have people who want to see their credit worthiness, so they select anonymized subsets of features of credit worthiness and they make the evaluations.

So are you thinking a similar idea could be applied here? For example, if we follow the same thing with SSAC if they want to somehow have an anonymization procedure that is taking place somewhere according to what they want to do (these are the requesters)? These trusted intermediaries, if I can say so, is the ones that are putting a security of a trust that their personal information will not be [divulged], will not be [forwarded], but the information that they need will be accessible. The feature, a pattern, that can [lead] to what they want (their request) – is this something that could help?

STEPHANIE PERRIN: If I'm taking your question correctly, there's a lot of work that can be done with non-personal data. There's also a lot of work that can be done with anonymized data, recognizing that there's no such thing as anonymized data. That will be probably in my

model. In one model, you would have all requests coming through here, and, in another model, only the requests that involve personal information because I think there's still a role for ICANN to have a great deal of data about registration publicly available, as it always has. You don't want to burden this rather expensive trust concept/think-tank with a whole lot of requests for anonymous data. That's not what we're trying to do here.

But the templating of the various requests coming through, and the verifying, indeed, that nobody is giving out any data unless it meets the requirements of a high standard – this is not just GDPR. You're going to harmonize, at a reasonably high standard, probably GDPR because it's the leader at the moment, although there are other isolated data protection laws that are higher, and manage these things. So that's what we're aiming for so that it is a kind of a front door through which the request for personal data come to ensure that we are not in non-compliance with the law.

Now, the registrars around this table a lot of competence in terms of data protection law. I'm confident they're doing a good job. The registrars who are not at this table, possibly some of the resellers through whom you work, are the guys I worry about. If ICANN mandates that the disclosure function must at least come through this front door, again, it still has to go down to the request, but then it goes back out through this door. Then you have an eyeball on what's going on.

Does that help? Does it answer your question?

GEORGIOS TSELENTIS: It was more to see whether – from your answer, as I understand it, you focus more on the decision … So you give the trust on the decision of the disclosure, whereas I was looking more for practical implementation of the use of the data that could be for anybody in this group that would lead to further automation also.

STEPHANIE PERRIN: So you're really looking for an analysis of the interest, yeah.

JANIS KARKLINS: Volker?

VOLKER GREIMANN: Two questions. First, this seems to be adding in a whole new layer of cost. Who's expected to pay for that? And what kind of staffing would you expect for that kind of trust that would have to be maintained?

Second question. It seems to me that, if you actually make that trust make those decisions, then the controller would essentially be outsourcing the decision-making to that body while maintaining the liability in-house. How do you take care of that disparity? Because potentially we would have to trust an entity to never make mistake or face the liability ourselves.

STEPHANIE PERRIN: Let's not kid ourselves. If ICANN does this, it won't be for free. So you've got costs if you involve any other outsourced party. I

consider ICANN an outsourcer here. But I agree. Costs are going to be fairly significant.

Hopefully it's governments. Here I giggle and laugh because I know how hard it is to get money out of governments who are cash-strapped. But I'm hoping we can at least get the data commissioner that will be sitting on this board in rotating thing to come for free that we won't have to pay. Good luck with that. Hopefully there will be some pro bono participation here without having to pay those individuals out of the funding of the operation.

It will be a joint controller relationship, as far as I can see, between the contracted parties and the trust. What I'm hoping is that that joint controllership will be more palatable than many other things of joint controllerships that we could imagine because there will be more trust and the liability will go down.

The model that I see would be quite differentiated. In other words, some types of requests would just remain with the contracted parties and other types of requests would be with the trust so that you would actually minimize their intervention. You don't want, as you suggested, [a] committee sitting here, thinking about every single request in the universe that is coming through. You want to streamline.

But for the difficult questions, I think it will reduce you liability to hand it over to a trusted partner.

JANIS KARKLINS: Any other follow-up questions?

If – Hadia?

HADIA ELMINIAWI: Thank you, Stephanie, for that. The idea or model as you have described here looks promising in many aspects, but as we [stand] now, you're still to propose the models. We don't know yet which model will go through. We don't yet anything about the funding. So when can we envision to have a concrete idea about a concrete model for what you're proposing?

Here I'm thinking about the time because we are all here looking at when are we going to finish this process in a good way and be able to implement it and have results out of it.

STEPHANIE PERRIN: As I keep saying, you can't make up for 20 years of inactivity on the privacy front in six months. This will take a while. This is a new concept. I don't think you're going to see this even in a model. Obviously I'll have some draft models by the end of the year, but whether those would stand up to a cost analysis is totally another question. But, quite frankly, I don't see the other model having a good cost analysis either. We don't have stats on how much volume we've got. I'm assured that, even though there are no requests right now, the request volume is going to just skyrocket shortly. We don't have good data, in other words.

To the extent that this solves problems, I think the request volume may go either up or down. How many serious requests have we got right now? I don't think you're going to see something solid with costing and funding potential for a couple of years.

Frankly, I haven't trotted this by our own government. I know that the data commissioners are interested. Obviously we're getting funded by them. I think it's a new concept in terms of how the data protection commissioners would look at this. But they're spending an awful lot of time looking at AI and algorithms, and all the other instances – I give you this [Carverfront] project in Canada with the Alphabet. That's almost a bigger and more pressing need in terms of solving this problem. We can limp along with the registrars running their own disclosure mechanisms until something better comes up. I don't think something better is a centralized model run by ICANN. So I think this still has potential.

JANIS KARKLINS: Thank you. Let's do Alan's intervention – the last one – and then we will do a family photo. [What do you think about that?]

ALAN WOODS: Thank you. I've been listening quite intently to this and I think this is definitely in the spirit of a good option because, when you start talking about this, to me it seems much more of a spherical standalone type of planet, in my brain, of that this is something that can absolutely pass muster by the DPAs themselves.

Also the fact that this is something that is a new envisaged path – there's no fudging of the concept of the [inaudible] as well, where you could ask for prior consultation. I think, again in the spirit of where data protection is and the principles it's based on, that we're trying to instill trust in this kind of idea and that they would be very receptive to the independent oversight review and probably would get involved with the nitty-gritty of it as well.

So, obviously it's years away and things like that. I just wanted to say that, as Option #3 and as a consideration, I find it exceptionally fascinating. Again, obviously it's theoretical, but I would be happy with that as a consideration going forward.

Another thing as well is … oh yeah. You were just saying the timeline for this and that obviously this is not something that would be created in a mere instant and the concept of hobbling forward with the way that it is at the moment. Yeah, I think that might happen anyway with the SSAD. We may have a longer period of trying to implement whatever that monster that could potentially come from that is. We're still looking at a timeline here that is unnecessarily long, unfortunately.

But what I would say to that is, again, even with the data trust as well, us as registries and registrars still will be answering those requests directly. We're just creating the easier path with a more trusted path. You can always still go to us as controllers because that is in the law that you can ask us for that as well. It's really not an option for us to say, "Hey, go to the data trust," or, "Wait for the data trust," or, "Hey, wait for the SSAD."

So, again, I jus wanted to say thank you very much. It was great to hear that. Actually, it was quite academically enlightening as well. So thank you very much. I appreciate it.

JANIS KARKLINS: Thank you very much. That brings us to the closure of today's meeting. Thank you very much, Stephanie, for sharing your thoughts and ideas with the team. You heard also the immediate

reaction on questions. Probably that will help you also fine-tune your own thinking about the concept itself.

With this, I would like to draw conclusions on our face-to-face meeting in Los Angeles. Thank you very much for your participation. As I mentioned, staff will now work on the 1.0 draft. That will be circulated as soon as possible. We will take it from there.

The Legal Committee meets next Tuesday. We are meeting tomorrow, right? We agreed. No. We are meeting next Thursday. The proposal for the agenda for Thursday's meeting will be circulated on Monday.

I maintain my open-ended invitation to those team members who would like to volunteer to do some write-ups for tasks that we still need to address. Where initial information maybe is not that sufficient, volunteer and provide input. As usual, the document will be published as a Google Doc. Every team member has a standing invitation to contribute in every way you think it's appropriate to the text that will be published.

With this, once again, thank you very much. Also I would like to use this opportunity on behalf of the team to sincerely thank the staff for the work that is done. By staff, I mean both the direct support staff of the team but also the larger indirect support staff of ICANN that makes our work as pleasant as it is.

So that's about it. Family photo now.

[END OF TRANSCRIPTION]