JAMIE HEDLUND: Morning, Ashley and Steve.

ASHLEY HEINEMAN: Morning.

JAMIE HEDLUND: Anybody else on?

ASHLEY HEINEMAN: I don't think so. It's just me.

JAMIE HEDLUND: Okay.

RAYMOND HO: Hello, this is Raymond Ho calling from Hong Kong.

JAMIE HEDLUND: Hi, it's Jamie. We'll give people a couple minutes to join. It seems like people are starting to roll in. All right, we'll get started, and hopefully more people will join. For the record, this is Jamie Hedlund. I thought I'd start off with just a quick summary of where I think we are, and then we can get into the discussion.

I sent out a discussion paper, which I'm sure many of you have seen. It points out that there is what appears to be a sharp division among IAG members regarding whether the trigger should be modified.

Registrars in the group have a voice that they don't believe it's appropriate to have to wait for some sort of notice from the government in order to request a waiver and it did seem to support the mechanism that's used in the data retention waiver process of being able to rely on opinion from a nationally recognized law firm.

On the other side, representatives of intellectual property owners point out that the [inaudible] requirement assures a credible demonstration of legal prevention which is required by the policy. And very generally to a high level, they don't agree that a law firm opinion alone would meet that threshold.

The short discussion paper sent out poses the question as to whether something or some things short of the notice from a government could satisfy the policy's requirement for a credible demonstration of legal prevention. So for example, expanding the available trigger or triggers. But at the same time, shoring up or better defining the verification requirements, some of which already exist, but some do not, so GAC member verification opinion from the ICANN General Counsel, which is also currently visioned, evidence of enforcement or intent to enforce and public comment.

So on the evidence of enforcement or intent to enforce, that would not necessarily mean evidence of enforcement against the petitioner, but just evidence that there's not only a law in place for regulation or

requirement, but there there is intention to enforce it either based on a history of enforcement or on evidence of intention of the agent agency to enforce it.

So that's where the paper is. But before we get started, I just wanted to remind everyone in this group following some of the recent exchanges of the mandate for this implementation advisory group, as described in the mission scope. As I understand it, this group is tasked with reviewing and potentially modifying the existing procedure in a manner that is consistent with the existing policy. The discussions today – the meetings to date have stayed within those bounds, and to me it would make sense to stay within those bounds until those discussions are exhausted, and then discuss whether additional recommendations should be included in any report from this group. We welcome feedback on that. Christopher? Christopher, are you there? You have your hand raised.

RAYMOND HO: This is Raymond Ho from Hong Kong.

JAMIE HEDLUND: Go ahead, Raymond.

RAYMOND HO: Yes, I think I already said my view is that basically in deciding, I agreed that we have to leave aside the policy questions, because as you mentioned, the mandate for IAG is to deal with a review on the existing situation and to see if there is a need for modification based on the existing policy.

Actually, that policy has been long-standing, as I indicated earlier today, that even the new gTLD, I think the same provisions is due. So [inaudible] policy, I agree that our focus should be on the triggers, but that the trigger – we should not exhaust situation where the trigger would be sufficient to demonstrate credibly the situation that by following the data public disclosure requirement that would give rise to an infringement with local legislation.

I think anything that satisfy on the balance of probability that such situations arises, would give rise to [inaudible] case. And the burden would then be on ICANN to rebut that [inaudible] case, to see if it has any force. If not, it can be disposed of. If it has a legal force, then it should be dealt with by way of a waiver on a case-to-case basis, or [inaudible] basis covering similar situation in a territory, a country, or a region where the related privacy data law or regulations will affect registrars or registries in the locality.

So I think the focus [inaudible] demonstrate on triggers, and we should not restrict those situations like legal opinion from law firms. Actually, some data privacy agency would offer rulings, and actually I'm not sure whether there was any in-house review undertaken by ICANN internally of the previous legislation worldwide.

Quickly, the situation in Europe may be different from the US, and so on. So it covers many possibilities and situations. So in a nutshell, I'm in favor of the [why], but a non-exhaustive list of circumstances that would give rise to a trigger. So that process, the burden to rebut the proof back to ICANN as a contracted party.

JAMIE HEDLUND: Okay. Christopher, I assume you're still not able to get on audio? Oh, I guess we'll . . .

ASHLEY HEINEMAN: I'm calling him now. He's having issues getting onto the call.

JAMIE HEDLUND: Okay. In the meantime, anyone else want to say anything? Okay. Steve?

STEVE METALITZ: Yes, thank you. First, I'd like to say I'm in agreement with you about the scope of this group. It's to consider whether there need to be changes to the procedure to implement this policy and doesn't get into the underlying policy.

Second, I saw Raymond's post earlier, I guess it was last night here. I don't exactly see this as an adversary situation necessarily between the contracted party and ICANN. At least, that's not how it's set up now, where one side has to make a [inaudible] case and the other side can rebut it.

I think instead, the goal is to vindicate the contract to the greatest extent possible, but where that's not possible, to make an accommodation. So that's where the credible demonstration of legal prevention comes in. If one party to the contract says, "Well, I know I've signed this contract, but I now have some credible evidence that I will

be in violation of local law if I do what the contract says," and at that point, again, under the existing procedure, the idea is for ICANN to get involved, to do a consultation, and do what it can to preserve as much of the contractual obligation as possible. And then potentially it could lead to a forbearance of enforcement of certain contractual obligations.

So I'm just not sure that I accept the model that Raymond is putting forward that once the registrar or registry comes forward with this credible demonstration, all they have to do is make a [inaudible] case and then there will be some rebuttal and then someone will – that assumes that someone, some tribunal will decide the question.

That's not actually what's involved here. This is something where all parties are assumed to be entering into a contract in good faith and with the intention to carry out their obligations, but one party says, "We've now found out that we don't think we can do that under our local law."

So that's a little bit different, and it does argue for having some pretty clear list or pretty clear criteria for what constitutes a credible demonstration of legal prevention. Thank you.

JAMIE HEDLUND: Thank you, Steve. Christopher, are you online now? Okay, Stephanie?

STEPHANIE PERRIN: Thanks very much. Can you hear me?

JAMIE HEDLUND: We can.

STEPHANIE PERRIN: Okay. We may have a terrible echo, but I'll do what I can.

JAMIE HEDLUND: If you're on the Adobe thing, you could mute your speakers. That might help.

STEPHANIE PERRIN: They seem to be muted already, but I'm still getting an echo. Maybe that's just my phone. What I don't understand – there's many things I don't understand, and let the record show I think you should change the policy. I think this is a nonsense, but I've already expanded on that in the list, I believe, adequately.

I don't understand. You have a letter from the Article 29 Working group, which is duly set up by a European directive. I mean, has anybody ever been before the Article 29 committee? Do they not understand what it is?

I've been before the Article 29 group. It's a very serious group of data commissioners. They're independent. They have made a determination in their working group, which is authorized by law to coordinate, and sent you a letter saying all of Europe has to be opted out here, and you're not accepting that. And nobody will answer the question, "Why?"

I did ask Steve Crocker when it first came, and I didn't really get an answer. But the only answer I have heard is that they aren't a "body with legal authority." Well, they're not a court and they are not per se the committee that a registrar has to come before, but the alternative is to get 26 letter – or, I'm sorry, I'm out of count here – 28 letters saying the exact same thing. I find this, quite frankly, rude. Above all, disrespectful. What more do you want? [Just to put that out there.]

JAMIE HEDLUND: Okay. Thank you. You've made that point on the list. Christopher?

CHRISTOPHER WILKINSON: Hi. Good afternoon, everybody. I've had to live with this issue for [inaudible] 15 years. I first discussed it with Paul Twomey when he was a chairman of the GAC. I've been a [inaudible] member of the GAC and secretary of the GAC in the intervening years.

Look, this has really been going on for too long. In the first place, it has been made very clear to ICANN not only by the Article 29 Committee – I thank Stephanie for her recollection of these details, but also by the European Commission, among others.

The contract is not legally correct in European jurisdiction. ICANN's Articles of Incorporation require that ICANN should respect applicable international and national law. The starting point is that. It's not what is currently in the contract.

Regarding Mr. Metalitz's point, there's absolutely no justification for waiting until there is an enforcement. I respect the speed limits before

the police car appears in my rearview mirror. It is inappropriate for ICANN and stakeholders to speak in terms of not respecting a law until you're threatened with enforcement. I think we should withdraw that.

You say that the policy is being fixed and we are only discussing the way in which certain aspects are implemented, but I would like to back up a little way. I've read the policy. The policy was recommended by a group of GNSO members, which as far as I can see exclude user interests and exclude governments.

We are not actually talking about the relationship between ICANN and its registry and registrar contractors. We're talking about the rights to privacy of the registrant. That is being systematically breached by this arrangement, so I doubt whether we could solve this problem without either amending the policy and/or amending the contract.

Finally, I read another document which speaks of the process for deciding whether or not a trigger should be awarded. It goes in six distinct steps. It could take weeks, if not months, to get through all of that.

Off the record, and I know this is being recorded, that reads like a monstrosity. That is totally . . . Yeah, insulting to people who want to respect the law. You have to prove six times over that you actually intend to respect the law which ICANN have been informed about for the past 15 years.

No, this doesn't give any credit to the ICANN system. To the point that you have said in several mails that the matter should be referred back to GNSO. Why? Actually, I don't think GNSO is fit for purpose in this

area. The relevant interests including law enforcement that should be present in such a decision are absent from the GNSO process.

I have no more confidence in the GNSO process, especially when it's dealing with matters which manifestly GNSO does not understand. I may return to the floor later in the meeting if necessary. Thank you.

JAMIE HEDLUND: Thank you. In response to both to you, Christopher, and you, Stephanie, again, what this group is tasked with doing is somewhat limited. And while you make important points, many of them are outside the scope of the mission and scope of this IAG.

CHRISTOPHER WILKINSON: Well, if I may interrupt you, Jamie, sorry, I read what you say, but this is not the first time that somehow or other that the staff or the board of the GNSO have circumscribed a consultation to the point that it has become futile. I've spent hours on another IAG with limited practical results because at every turn, somebody says, “Ah, but that's not in the mandate.”

Could you please confirm that there is not in effect a significant desire by the ICANN legal department or other stakeholders to make sure that the mandates are drawn so narrowly that we're all wasting our time?

JAMIE HEDLUND: No, I can't.

CHRISTOPHER WILKINSON: Why should I spend time on—

JAMIE HEDLUND: And I won't. But I will say is that the structure, the work of a multi-stakeholder community is often structured by mission and scope. If there's a problem that comes up in a particular working group or IAG or within the GNSO that's not covered by that mission and scope, then it needs to be brought up somewhere else.

We would love to solve peace in the Middle East, but we're not going to have that here. We're not going to solve peace in the Middle East, but were not going to solve that here.

CHRISTOPHER WILKINSON: Jamie—

JAMIE HEDLUND: It's the same thing.

CHRISTOPHER WILKINSON: Maybe go back to first principles. Who is the chairman of this working group?

JAMIE HEDLUND: There is no chair.

CHRISTOPHER WILKINSON: I do not accept a meeting that is conducted exclusively by the ICANN staff. We need a chair. We need a chair that is neutral, and preferably from outside GNSO.

JAMIE HEDLUND: This is not a policy-development type working group. Implementation advisory groups don't work this way. If the group wants to structure itself to have a chair, that is perfectly up to the group, but it is not by the fiat of one person, ICANN staff or otherwise.

CHRISTOPHER WILKINSON: I rest my point.

JAMIE HEDLUND: The area, Christopher, that you did raise which is very much relevant to this group is whether or not a registrar or registry has to or can't avail itself of an exemption unless and until it's subject to some sort of legal notice, and so that fits well within the scope.

And then secondly, to respond to a comment that James Gannon raised on the chat and has been said in the e-mail exchanges, it is well within this group's mandate to recommend a revisiting of the policy of the GNSO.

CHRISTOPHER WILKINSON: Okay, but not by GNSO. Not by GNSO. We've had enough of that.

JAMIE HEDLUND: Well, the GNSO is the policy-making body. I'm sorry?

CHRISTOPHER WILKINSON: I think we've had enough of being led by the nose by GNSO, which has been demonstratively either ignorant of the matters that they're dealing with, or perversely obstructionist. Let's see . . .

JAMIE HEDLUND: Well, that sounds like you have an issue with the structure of ICANN, which again, which again is outside the scope of this group.

CHRISTOPHER WILKINSON: I together with Ira Magaziner, I'm responsible for the structure of ICANN. Don't [inaudible].

JAMIE HEDLUND: I don't know what to say to that.

CHRISTOPHER WILKINSON: You don't – no reply is required.

JAMIE HEDLUND: Excuse me?

CHRISTOPHER WILKINSON: No reply is required, Jamie.

JAMIE HEDLUND: Yeah. But again, this group cannot work on the bylaws that describe what the GNSO is tasked with or not tasked with, and we have to work within the realities of the ICANN structure as it is and the mission and scope as it is to the extent that there are bigger issues to discuss, those need to be raised, also.

CHRISTOPHER WILKINSON: [inaudible] responsibility legitimately of GNSO. It is quite clear that the personal privacy of individual registrants is not. That's the bottom line, Jamie. This is not a matter that's between registrars and registries and ICANN. This is a matter of respecting the law as it applies to the individuals.

RAYMOND HO: Jamie, if I may?

JAMIE HEDLUND: Yes, Raymond. If you could hold, Volker's had his hand up for a while.

RAYMOND HO: Okay.

JAMIE HEDLUND: And then we'll go back to you. Volker?

RAYMOND HO: Thank you.

VOLKER GREIMANN: Yes. Volker Greimann GNSO Council vice chair and counselor for the registrar for the stakeholder group, speaking in my capacity as a GNSO Council member here, I believe that the question of the policymaking for the process could indeed be a GNSO process.

However, I would agree that the question of what law to respect and privacy law in general is not as such within the GNSO remit. That's a matter of respecting the laws that stands, and any working group working within the GNSO would have to take into account the laws that would apply to the subject matter at hand. In this case, privacy laws of the different countries.

So I would disagree with the statement that this is not a GNSO matter. It very much is a GNSO matter that would have some remit within the GNSO, but the GNSO would not be free to make up policy as they go along. They would be working within very strict requirements, i.e. having to respect what the law is and implementing that into policy. Thank you.

JAMIE HEDLUND: Okay. Thank you, Volker. Raymond?

RAYMOND HO: Yes, I have two points. Thanks, Jamie. Point number one is what I am advocating is not an adversarial approach to the issue. What I'm suggesting is that the burden to demonstrate credibly the situation by the registrar could be many so long as – and I don't think that we should confine to situation where there is actual enforcement or notice to enforce.

So it can be dealt with under the ICANN Registry Agreement by way of consent between the ICANN and the registrar so long as the trigger has been demonstrated, and ICANN should respond reasonably to address their concern. So it's not a [contentious] approach. It's a consent approach, rather.

Number two is that actually if you look at the Registry Agreement Schedule 4, it is written in a pretty flexible manner. If I may read from the latest version of the new gTLD Registry Agreement, Schedule 4? Right at the top of Schedule 4, there is a – let me turn to that page, which is on 63. Page 63, if I recall correctly.

Now, the first paragraph of the Schedule 4 demonstrate the [inaudible] flexibility, which ICANN already adopted. It starts with the words "Until." Schedule 4, clause 1: Registration Data Directory Services. It says, "Until ICANN requires a different protocol, Registry Operator will operate a WHOIS service available via port 43 in accordance with RFC 3912, and a web-based Directory Service at <whois.nic.TLD>, providing free public query-based access to at least the following elements in the following format."

Then it goes on, “ICANN reserves the right to specify alternative formats and protocols, and upon such specification, the Registry Operator will implement such alternative specification as soon as reasonably practicable.”

Now, my point is, [inaudible] about privacy data, the standard requirements under the WHOIS service, public service, will require a number of things: the name of the registrant, and I think the name of the registrant may or may not give rise to privacy data concerns. But the address of the registrant, the telephone number of the registrant, the fax number of the registrant, the e-mail of the registrant, those may be affected by privacy data sort of regulation in some jurisdictions, maybe in Europe in particular.

So the [inaudible] trigger may not give rise to a complete shutdown of the WHOIS public database, but only certain items will not appear in the public domain. Now, actually that's a flexible arrangement which already incorporated in Schedule 4, which ICANN can, if satisfied that triggers has arisen, to modify the scope of the disclosure so as to comply with territorial or local privacy data requirements. So this is my second point. Thank you.

So that brings me back to my first point is that when considering trigger, we should leave it as wide as possible. Like the Article 29 [inaudible], that should sufficiently demonstrate a situation has arisen.

So it's a matter of consent by the registrar and ICANN to work on modification, particularly what the existing provision is available for

ICANN to give appropriate modification of the WHOIS service scope so as to restrict the likelihood of infringement.

JAMIE HEDLUND: Okay, thank you. Two hands are up, Stephanie and Steve. Stephanie, please go ahead. Are you on mute, Stephanie? Okay. Steve, go ahead.

STEVE METALITZ: Yeah, thank you. I'm looking forward to having some discussion about the trigger, but since so many other issues have been raised, I guess I just want to make two points. One, as Mary Wong as indicated in the chat, the policy that we're talking about here was a recommendation – I believe a unanimous recommendation – of the GNSO council. It was adopted by the board, which directed the staff to develop this procedure. The procedure was put out for public comments and I think it was slightly modified as a result of that, and then the procedure was adopted.

We're being asked to review the procedure, which is in line with the terms of the procedure, but the suggestion that there was something [inaudible] about the process or that [inaudible] interest didn't have the ability to be heard, I don't think is [worn out] by the facts. Anyway, that's where we are.

I don't know exactly to whom Stephanie's question about the Article 29 group was directed. I suspect it was directed to ICANN, and obviously I can't speak for ICANN, but I guess to pick up on what Raymond just said, I think the reason why a letter from the Article 29 committee in general

terms denouncing the ICANN contracts or the ICANN WHOIS policy is not a credible demonstration that any particular registrar is legally prevented from fulfilling their obligations under the contract because the Article 29 Committee is not an agency that enforces any law.

And if an agency that enforces any law tells the registrar that they do what the ICANN contract requires, they will be in violation of that law, that comes much closer to the credible demonstration of legal prevention. [inaudible] of the Article 29 Committee, while I recognize that it's composed of experts and people that have a lot of knowledge and authority within their member state, within their individual countries. When they're acting as the Article 29 Committee, they have no enforcement authority.

And therefore, that's not the legal prevention that the policy demands. That's my response. I don't know. As I said, I can't speak for ICANN on this, but that's how I would interpret it. I'm happy to get into any – Jamie's paper put a few different alternatives out there for how in the absence of the enforcement action, you could find the trigger and be happy to discuss those when the time comes. Thank you.

JAMIE HEDLUND: Yeah, thanks. I will only say that the European Commission at a GAC meeting also raised the issue of the authority of the Working Party. And had there been – a letter from a DPA, in this context, would for sure be treated differently than a letter from the Article 29 Working Party.

All right, Stephanie, can you talk now?

STEPHANIE PERRIN: I hope so. I think you've unmuted me. Can you hear me?

JAMIE HEDLUND: Yes.

STEPHANIE PERRIN: Good. Well, I believe Jacob Kohnstamm did write back. That would be the chair at the time of last summer's [inaudible] with the Article 29 group. He did write back and say, "Would you like letters signed by all 28 commissioners?" So a response to that might be nice.

I don't wish to belabor this point. I understand that we are – it's an odd working group, but it appears to be only interested in [inaudible] concerns about the difficulties in enforcing this policy that the registrars have been facing, so I'll do my best to bring it up at the GNSO.

I have concerns as to whether it is within their agreement to decide whether to follow a law or not, but if that's the process that put this beast in place, then obviously we'll have to go back to the process that put it in place.

However, I do think that the way this policy is being administered, which is within the remit of this committee, causes the reputation of ICANN to be put into disrepute. I mean, really, if you are forcing – I see that Mary has put in the chat something about standards of law. The problem with data protection law, and having been the policy director drafting one – I believe I have some authority here – you put things into

a law, you have to wait until they are litigated to get a final determination.

I give you, for instance, the “right to be forgotten” case that just went through the European Court of Justice. Now, anybody who's worked in data protection, and it appears that there is a bare minimum of those people at ICANN, knows full well that an individual always did have a right to request the rectification and deletion of information. The issue of whether they could force Google to do it or not if Google decided it wasn’t going do it, even though it would do similar takedown notices for intellectual property owners, that had to be litigated.

How many years has it taken? That provision has been in the Spanish law since it was brought into force. Quite frankly, I can't remember when that was – not as long as France.

So what ICANN is doing in an industry that is basically formulated on a first past the post market model to get domain name registry, what you're basically forcing anyone who wishes to enjoy the protection of data protection law to do is to go to court and get a case.

Now, how is that sound, accountable policy in the public interest? I can give you five reasons off the top of my head why it is not in the public interest to take up court time litigating these matters when you have plenty of evidence that it violates data protection law. This is just nonsense.

And so to have us persist in working on something that is fundamentally not in the public interest is, I would say, a violation of the ethical terms under which ICANN operates. Thank you.

Plus it puts, as I said, I think repeated in my post on the list, it puts the registrars at risk. If the only way I can get this enacted in Canada is to litigate, then I'm going to have to mount a crowd-sourced campaign against all of the registrars in Canada.

Now, American registrars might be pleased with that, but I don't see that that's in the public interest, nor is it fair to any country that doesn't have a system such as the Article 29 group to collectively represent the interests of their region. Thanks.

JAMIE HEDLUND: Thanks, Stephanie. Volker?

VOLKER GREIMANN: Yes, Stephanie is exactly right, and it goes even further. I mean, you know the European Union has the opinion, and I think rightly so, that any company, be it a European company or a foreign company that handles data of European data subjects is subject to European data protection laws. So if you have an American registrar that has European customers, it has to protect, according to the letter of the law, the data according to the laws of Europe so he wouldn't be able to – he would have to have a special system for his European customers, and not many do.

This has not been litigated yet in many cases. However, this is what the law states, so there's a whole problem that has not even been addressed yet. But that wasn't even the point I was trying to make.

I think you said earlier that if a data protection official would be coming forward and giving you a statement to the effect that a certain practice would be legal that you would act upon it, now I know for a fact that, for example, Luc was also here, had the problem that they sent for their registrar a letter from their Luxembourg data protection official, and they face the exact same problem that those registrars that were in a different jurisdiction faced when they presented the law firm's letters of opinion.

And finally, I would like to just state that while the Article 29 working party is not in itself a legislative data protection body that has any authority, its members do, and I would at least see them on the same level as a law firm that provides opinion on overall European level.

So why this was always rejected by ICANN was frankly puzzling to me, so it was my opinion and my viewpoint that it seemed to me that ICANN was not treating this as it was intended, i.e. a fair arbitration process where a registrar could come or registry could come and say, “Here we have this problem. Can we please be exempted?” And ICANN would say, “Make senses. Okay.” But rather as seen as a negotiation because ICANN was afraid to lose face if they granted this provision because there were powerful interests involved that just simply did not want this exemption to take place.

So when we came with a letter that said a certain amount is not possible, we need to have it limited to a certain/different amount of time of storage, then ICANN came back with, “Can't we do this time? Can't we do middle ground in between?” And that's not what the letter of opinion said. That's not with the data protection officials said. That's

not what the Article 29 data protection group said, but that's what ICANN asked for with no legal basis to back that ask up, so it seemed very much like a negotiation.

And this is not a negotiation. This is a question of what is allowed on the law, and that cannot be negotiated between two parties. It has to be found out, investigated, and then accepted.

JAMIE HEDLUND: Sorry Thank you for that, Volker. I was talking into – muted my telephone. Ashley, you're next.

ASHLEY HEINEMAN: Yes, thank you. I'm glad to see we're kind of getting back to what we had intended to talk about today. I was worried that we'd run out of time before getting to that, so I wanted to get in the queue and just state that I think while we weren't all on the same page, I thought that based on our last call, that we're getting to a point where the group was willing to discuss additional potential triggers, as well as what kind of verification was required to allow such additional new triggers.

And one thing that I believe I mentioned on the last call, but I'm not sure I did, so I wanted to do so here is that recognizing what Steve had said via e-mail that, as of now, the existing procedure already builds a GAC review process. But my understanding is that the one time that that was actually utilized, it couldn't be because there was a non-disclosure associated with a letter they had received from the party.

So I was wondering if we just kind of go down a route of having additional triggers but kind of looking at the existing ones, as well, is there a way that we can deal with those situations where you can't really verify because the information that's been provided is not allowed to be disclosed?

JAMIE HEDLUND: Thanks, Ashley. I mean, it seems like that's a little bit like the scenario in which the jurisdiction does not have a GAC representative, so it can't be verified that way.

So the question I have is whether it would make sense to talk about acceptable means for verification, which would – because it seems that it comes down to, how do you verify that the information is correct and it comes from an authoritative source? Because if we do that, it might be easier than to craft additional triggers. But that's just a thought, and I welcome other people's input.

All right, Stephanie?

STEPHANIE PERRIN: With respect to the question of whether the GAC representatives are the appropriate people to make a determination about whether something is authoritative under the data protection law of the country, I must say I'm a little skeptical having heard while of the biggest case in Europe being litigated that the Court of Justice, namely the Spanish one on Google – the Spanish representative asked, "How on Earth do we find out who our data protection officers are?"

So I would suggest to you that many countries might be ill-informed and not necessarily know what's going on. Maybe if you're going to accept the advice of a GAC representative, you have to at least ask them to bring a letter from their Department of Justice indicating that the authority was the authority.

The problem there is the governments are often in litigation with the data protection commissioners over data protection laws, so yes, sure, they're the [inaudible] representatives, but I don't quite understand why a letter from a data protection authority isn't good enough, you know? It's the difference between government and separate legal authority, a court. Thanks.

JAMIE HEDLUND: Well, we had talked on a previous call – someone had mentioned the possibility of the effectiveness of a letter from a DPA, and I can't remember if it was Michele or someone else who brought up the fact that DPAs are not in the habit of writing opinion letters, but a letter from a DPA would certainly be something to consider as a verification measure. Steve?

STEVE METALITZ: Yes, I would agree with Stephanie on this point that there's nothing about the GAC representative that automatically changes something from not meeting the credible demonstration of legal prevention threshold to meeting that threshold. So I think what – as I understand what your discussion paper is about, you're assuming that there's something – let's say a letter from a law firm, and we could get into

what that actually says, but let's say there's a letter from a law firm and raising questions about this, about the compatibility of the contractual obligations with the data protection law.

And that is not currently enough to satisfy the trigger, and you're asking whether if that letter were referred to a GAC member and they endorsed it, I guess, would that be enough to constitute the trigger? And I think for the reasons Stephanie was mentioning, it wouldn't necessarily.

If what they come back with is something that says, "Yes, we've looked at the letter. We have also looked at the law and at the terms of service that the registration agreement, in which the registrar has consented to disclosure this information, and we've looked at all of these factors, and our data protection authority has said that this is not satisfactory. This is a violation of our law." That's one thing.

But just simply the GAC member saying, "Yeah, I agree with this letter," GAC members are from all different agencies, some of which may have some relationship to the enforcement of the data protection law, but many of which don't.

So again, it doesn't seem that by itself, what the GAC member says – the GAC representative, I should say – says is enough to take something that isn't a credible demonstration and make it a credible demonstration. Thanks.

JAMIE HEDLUND: All right. Thank you, Steve. Anyone? Ashley, you're up.

ASHLEY HEINEMAN: This is kind of skewed a little bit from my original question, but I am agreeing with the previous two people who spoke to this issue. And I also want to take it a step further in that multiple layers of verification might be required, whether because you need multiple layers or your first layer just wasn't able to answer it or wasn't sufficient.

And I'm not sure there is one – it's possible to have one definitive way to verify if the trigger is coming from a party that's not the relevant government official or government agency. I would think that there might need to be, as I said before, kind of multiple layers, whether it's you have the GAC review, you have the public comment process that you talked about previously, in addition to having some kind of internal ICANN review if you all decide to take on some sort of a privacy expert.

JAMIE HEDLUND: Yeah, but I took Steve's point to mean that even an opinion letter from a DPA might not be enough because they may be in the middle of a litigation or some sort of dispute domestically with other parts of their government.

STEVE METALITZ: I don't think that I said that. Maybe somebody else. I think Stephanie said.

JAMIE HEDLUND: All right, Stephanie?

STEPHANIE PERRIN: Thanks. If you were referring to my remark about how governments are often litigating with the data protection commissioners over points of law, that's what I said. What that does is merely point out that by asking the GAC representatives, you're not necessarily asking the independent authority. You're asking someone who could be a party to a case, okay?

So, I mean, this is why this whole thing is completely crazy-making. Any data protection authority that has binding powers that would have the power to write an order is not likely to send you a letter for the simple reason that they have quasi-court functions, and they might even be actual court functions.

And they're treated like judges in our country. They're paid as judges. They follow the same rules, whether they've got the binding powers or not. You're not likely get a letter.

Now, I checked with the data commissioner yesterday. And to the best of her knowledge, nothing has come before any of the commissioners on this matter. That brings me back to ICANN forcing a jurisdiction, or those in the jurisdiction who care about living under data protection law, to litigate. And unless you tell me that there's some other system that we've come up with here that will obviate that, that's what we're stuck with.

JAMIE HEDLUND: Stephanie, that's exactly what we're trying to come up with. We're trying to see if procedure as it exists, which requires a notice, can be modified in a way such that something less than a notice is a trigger so long as there is adequate verification measures.

STEPHANIE PERRIN: And what do you mean by a verification letter layer? I mean, this just sounds like something that is definitely not in the public interest if you have to find six ways to validate a very simple point. And in terms of—

JAMIE HEDLUND: [inaudible]

STEPHANIE PERRIN: I can give you a letter tomorrow that says, “In my view, this matter is outside Canadian law.” I can get a former commissioner to sign that letter because she's not a commissioner anymore, right? Are you going to accept that? No. I'm just one privacy expert. I'm not even a lawyer, so that doesn't count, right?

JAMIE HEDLUND: So maybe it would be helpful to point to what the policy calls for, which is the development of a procedure for dealing with a situation in which a registrar or registry can credibly demonstrate that it is legally prevented by local/national privacy laws or regulations from fully complying with the WHOIS obligations. So . . .

STEPHANIE PERRIN: But at the risk of beating a dead horse here, Jamie, this is what I think what Christopher and I are on about. If the policy – if what we have set up here is, I don't know what the word is. Tautology? Is a non-provable

argument, then have embarked on something that is going to put ICANN in disrepute. This is crazy.

JAMIE HEDLUND: Well, with all due respect, putting ICANN in disrepute is not a new thing.

STEPHANIE PERRIN: Well, that doesn't mean we should continue to do it. I'm not volunteering my time for nonsense.

JAMIE HEDLUND: But what is relevant, again, here is I don't see that this is a tautology. There is a requirement from a policy that's been developed by the community. Those are the WHOIS requirements. Those go into contracts with registries and registrars.

There is acknowledgment that there may be laws or regulations that conflict with that, so how do we figure out how to, as policy requires, enforce the WHOIS obligations to the maximum extent possible, but at the same time build in some sort of exemption for those jurisdictions where it conflicts? And so that's what we're tasked with coming up with, a policy that allows someone to come in and say, “I can't comply with this policy, and here is my credible demonstration of legal prevention.”

And so what we're trying to do here, I think, is come up with what are the possible elements of a credible demonstration of legal prevention that would allow for an exemption from a contract revision?

STEPHANIE PERRIN: I understand that, Jamie, but if the proposition is . . . Because due to the nature of extraterritorial application as the law, let me tell you that all I would have to do, in my opinion at least, which is only one opinion, is register a domain in every single jurisdiction, whether they're represented at the GAC or not, and complain everywhere.

And that's kind of what we're driving to because if we wait for every single country to have a complaint to turn down a policy that globally is unacceptable, the only way to do it is to crowdsource it. That's what I mean by bringing ICANN into disrepute. If that's what you're pushing towards, then this is really reckless, you know?

JAMIE HEDLUND: Well, ICANN is a global organization and the contracts apply globally. They do not include the laws of individual jurisdictions. They do require compliance with local jurisdiction, but they don't say, "This is the law of the United States and therefore you shall comply with it."

So what we're trying to do is to reconcile the difference between national jurisdictions and a global vehicle that the ICANN community has developed for its agreements with registrars and registries. And so if there were a uniform law around the world that made the collection of WHOIS information illegal, then we wouldn't be having this discussion, but that's just not the way the world is right now. And so we're looking for means of providing relief where it's demonstrated that relief is justified.

CHRISTOPHER WILKINSON: I'm sorry, but that's nonsense. I mean, just because ICANN is an international organization, it still can't still take into account national laws. It must take into account national laws for those registrars and contracted parties that are bound to those national laws, and it needs to find a way to make an exemption for those registrars that are bound to national laws to enable them to do business. [inaudible].

JAMIE HEDLUND: And that's exactly what we're trying to do, find a way of doing that.

CHRISTOPHER WILKINSON: Yes, but in a way that works.

STEVE METALITZ: Could I get in the queue here? I've had my hand up for a while.

JAMIE HEDLUND: Yes, please. I'm sorry, Steve.

STEVE METALITZ: It's okay. Two points. First, on Stephanie's point, it may be true that in some countries, data protection authorities only speak when they bring enforcement actions, but that's certainly not true in every country. And in fact, ICANN has received opinion letters from data protection authorities regarding WHOIS and has acted on them in the past.

I think that those opinion letters have been made public, and I think that ICANN misinterpreted the letter from the Spanish data protection authority in the case of .CAT. But be that as it may, there was such a letter ICANN did act upon. It didn't do it through this procedure, which I think it should've done. But for whatever reason, ICANN has been extremely lax in how it has applied this procedure in the case of registries.

My second point, I wanted to get back to the discussion paper that Jamie circulated and something that he said in his introduction. Because he had several potential verification requirements, and one of them was evidence of enforcement or intent to enforce by the relevant government agency. And when I read that, I said, "This kind of sounds like the existing policy." I wasn't quite sure what the difference was here.

And then I believe he said in the introduction, "Evidence that there is not only a law in place, but there is intention to enforce it." So I'm not clear exactly on what, Jamie, you meant by that, but maybe others have a clearer understanding than I do.

Again, take the situation in which there is a letter from a law firm that raises concerns about the compatibility of a data protection law and its applicable in the contractual requirements. And so the verification process would be evidence of enforcement and intent to enforce by the relevant government agency. I'm just not clear on what that means or how that's distinct from the status quo.

JAMIE HEDLUND: So, Steve. Christopher, I'll get to you in one second. I just want to quickly respond to Steve if I could. I mentioned this at the top of the call, but this was an attempt – this was an idea of verification means that didn't require direct enforcement against the petitioner, but it would be a further indication that there is a law in the books and it is enforced.

So it could be enforcement action taken against somebody else. It could be a statement by the DPA that they have this law, this is what it means, and we will enforcement. It gets to the issue of speed limit signs, which exist, but may not be – there's [prosecutorial] discretion. They don't bust everyone who breaks the speed limit, but it is nevertheless a binding regulation.

So it was an idea just to expand the notice requirement now beyond that to some sort of evidence that not only is this law in place, but that it's enforced. Does that make sense?

STEVE METALITZ: Yeah, I think that that's helpful. Two situations that you described. One is the data protection authority saying, "This is our law, this is what it means, and we will enforce it." I think that under the current policy, assuming the data protection authority is the enforcement authority, I think that qualifies under the existing procedure.

[inaudible] enforcement being brought against somebody else, that's a good point. So if you have two registrars in the same jurisdiction and the data protection authority brings a case against registrar A and registrar B, again, the gTLD registrar was subject to the same

requirements on WHOIS. It comes to ICANN and say, “There’s a credible threat here. There’s a credible demonstration here because registrar A is being sued by the data protection authority.”

Yeah, I think that – again, that's a little different from than just saying, “Well, here's a law that has something to do with their protection, and therefore we would like to have this waiver.”

JAMIE HEDLUND: Okay, Christopher?

CHRISTOPHER WILKINSON: Yeah, thank you. The conversation has been quite interesting. Allow me to refer back to my earliest posting on this matter. I'm not in favor of exemptions. I regard that as a last resort because of the curiosity of ICANN’s policy. What I really want is for ICANN to respect best practice of privacy law worldwide, irrespective of the jurisdictions, including the United States.

All this talk about enforcement makes me very uncomfortable. The starting point surely is that registries, registrars; and indeed, registrants, respect the law. You don't go around saying that the companies and the general public can do what the hell they like unless they're personally threatened by enforcement. Enforcement must be the exception, so I think the conversation has identified two or three reductio ad absurdum.

And since it's past 4:00 and I have to go and make lunch for my family, I would invite the staff to consider what they've heard today and produce

another working paper, a working paper which is just about triggers. It risks wasting a lot of time.

Now, just to fill you in on the European situation, there is a negotiation going on between the institutions and the member states, the results of which could well be that, in future, European privacy law will be regulated by what we call a regulation, which is a directly-applicable European law, whereas the present situation is a directive which is implemented by each of the member states, albeit in some respects differently.

So if that comes about within a foreseeable time horizon, ICANN will be dealing with a sole authority dealing with privacy law Europe-wide. So digging ourselves into this absurd situation of wanting to get information about enforcement and credible [whatsit] of country by country, registrar by registrar, quite apart from the absurdity that's already been described, it's a temporary solution, if that. So please, could we get real? Could we get real? Could the staff please withdraw your paper and start again?

JAMIE HEDLUND: Happy to take ideas on how to – what to include in a paper that's within the scope of this group's work, which includes making recommendations to GNSO to revisit the policy. Stephanie?

CHRISTOPHER WILKINSON: Just as a footnote, Jamie, who the hell wrote the scope? I mean, anybody who's followed this issue superficially in recent years must have twigged that this scope was inviting refutation. Who wrote this?

JAMIE HEDLUND: The scope derives from the original policy in part six, I refer you to, which calls for review of the procedure annually, and so that's what we're doing.

CHRISTOPHER WILKINSON: Right. Right.

JAMIE HEDLUND: The policy was developed by a community.

CHRISTOPHER WILKINSON: Just go back on the record that as far as I can see in this particular case of the subsets of GNSO, who seem to have invented this, didn't know what they were talking about.

JAMIE HEDLUND: Okay. Thank you. Stephanie?

STEPHANIE PERRIN: I've already said this, but just in case nobody read it, I just want to say that at least in Canada, enforcement is a major problem because if the privacy commissioner investigates a complaint – let's say I complain

about let's say [Two Cows] – [inaudible]not on the call, you snooze you lose. If the commissioner writes a letter to [Two Cows] saying, "I believe you're violating the data protection law," and [Two Cows] chooses to ignore it, then in order to enforce that, he has to take that case to the federal court. Change of commissioner.

Now, and that covers nine of the provinces – ten – because she's acting for nine of them. There are three that will act in their own interest, and who knows how they're going to find. Obviously someone who complains will be doing it in all territories and provinces, so you're imposing on the Canadian legal system 14 separate cases that I would have to take, right?

But the commissioner has very limited resources. This was not set up like traffic cops, you know? She has to pick and choose which cases she's going to take to federal court, and she has to do it within a timeline.

This is what I think is putting ICANN in, I would say, moral disrepute. You're playing a game of chicken with the data commissioners because many of them are in this situation. They have to take it to a higher court to pursue the matter. And really, ICANN isn't top of mind for these guys, and why should it be?

So that forces. You're still violating the law, but you're demanding an enforcement action that really –well, it's there, ICANN isn't going to meet the threshold. I can complain to my county about the fact that there is litter along my street when I walk my dog because I live in the country, but they're not going to send out an enforcement officer just to

stop litter landing on my street. That's exactly the parallel here. That's why this process has to be reconstituted. Thank you.

JAMIE HEDLUND: Thank you. James?

JAMES GANNON: So as much as I could happily go along with Stephanie for many hours on just the fact that this is way out of whack, I think we have two things. We have, one, I think we need to start working on a recommendation to the GNSO to possibly revisit the policy. So there seems to be a lot of people in the group that want to do that.

So we have two things that the group needs to do as far as I can see. One, we need to start working on possibly asking – making recommendations to the GNSO to revisit the policy, which I will also note is ten years old now, and a lot has changed in the data protection laws over ten years. So possibly it is time to do that anyway. This may be the catalyst to do that.

And secondly, we also have on the procedure side, we have this issue of enforcement and enforceability. I think there needs to be a certain amount of compromise from ICANN's side in realizing that the default under national law should always be compliant with law. Having a requirement to show that a national law is enforced is very, very difficult.

[inaudible] a situation in the chat that the data protection law brought in, for example, European states. I'm a European, so I'll use that

example. And as should be the case, the law is obeyed, so therefore there has been no enforcement actioned. Are we now really going to say that ICANN will not recognize that law's applicability to the exception because it is being obeyed?

So under that, I think we really need to sit down and have a look at the procedure and how we can address the enforcement issue because requiring a member of a state to [approve] enforceability of their national laws, I don't believe is a realistic situation going forward. It's not in line with any other contracting party that I've ever dealt with before.

My experience running a number of companies, and I think we need to be quite realistic and come to a realistic compromise between what ICANN wants, and I understand that side of it, but with the acceptance that the default status of a national law or that of a Data Protection Act is enforceable, if not enforced.

JAMIE HEDLUND: Thank you very much, James. Just one quick clarification: ICANN doesn't want anything. ICANN is facilitating this IAG for the purpose of the IAG recommending changes to the procedure and any other recommendations to the GNSO that it may wish to do. We do not have a position on how it should be changed, what it should be changed to.

Again, we're merely facilitating the discussion. The idea of enforceability or evidence of enforceability was one that was thrown out and can be rejected by this IAG easily. It was an idea to respond to the need expressed by others for verifiability.

It sounds like you believe and others that it's a bad measure for all kinds of reasons. ICANN's absolutely fine with that. The task for this group is to review the procedure and come up with suggestions, if necessary, to revise it. So I just want to make clear that ICANN does not have a position on this.

And Volker, please do not interpret what I'm saying as a desire for inertia. There's been too much work put into this and other matters to suggest that ICANN doesn't care or doesn't want to see changes implemented that are desired by the community.

Okay, Steve?

STEVE METALITZ: Thank you. I have two comments on this issue of policy or the procedure. First, Christopher raises the point that, to the extent this is an issue about European data protection law, which it is obviously not the entire universe here, and I'm sure Stephanie would point that out, but it's a big part of the issue. And to the extent that there are going to be changes or there may be changes in European data protection law, including enforcement at a transnational level, not at the national data protection authority level, which is the status quo now, it might make sense – I mean, to me, that argues for not changing anything now.

If the European situation is going to change, then ICANN is going to have to react to that or adapt to that. That may well need to require changes in how this procedure is implemented.

So those who are closer to the situation in Europe can have a lot more insight into this than I do. But if the law's about to change there, then I think it would be kind of a waste of effort to make dramatic changes in the procedure that would, again, have to be revisited rather quickly.

My second point is I understand that a lot of people on this call want to change the policy. I think it's quite clear that this group does not have the authority to recommend a change in the policy. It's outside the scope of this group, and there are avenues that I know Stephanie as a GNSO counselor and others are well aware of the avenues that are available to try to start a policy development process or a commission an issues report and so forth to change the policy. It's not within the scope of this group, in my opinion. Thank you.

JAMIE HEDLUND: Okay. James?

JAMES GANNON: From previous discussions that I'm aware of – I only joined this group recently – I believe that making the recommendation is most certainly within scope of the group. I've had staff agreed with me on that. Changing the policy is not, but making the recommendation to the GNSO to revisit the policy and possibly giving some issues scoping around that, I believe that is definitely within the scope of this group.

[UNIDENTIFIED MALE]: I agree with you.

STEVE METALITZ: Can you point me to where in our mission and scope statement that possibility is [addressed]? I don't see it.

JAMES GANNON: Well, one of the issues around implementation of any policy is that the implementation may be unfeasible, and the recommendation on how to continue the implementation of the policy can be to revisit the policy.

STEVE METALITZ: [inaudible] look at that, then I agree that would be in scope, but that GNSO did not include that.

JAMES GANNON: That's my understanding of the role of the group.

STEVE METALITZ: I disagree.

JAMES GANNON: I'm sure it won't be the first time.

JAMIE HEDLUND: It would seem to be a logical possible outcome that the work of this group does include a recommendation that the GNSO reconsider this. Obviously, that does not trigger a PDP. It is just a recommendation of

what this group has decided, and it would have to include the rationale for why this group believes that the policy should be revisited.

All right, no one seems to have their hand up, so at this point, we've only got two minutes left by my clock, and so I thought maybe it might be time to figure out what we should do for the next call and what we should do up until then. One thing to consider would be to have a discussion about what additional triggers and verification measures might be good for what other potential modifications to the procedure would be worth considering.

I hope that there's a better understanding following this call about in terms of what's in scope and what's out of scope. What's out of scope doesn't mean that, obviously, that they are issues not worth considering, just that this is not the right place for that.

Anyone have any other ideas about what they would like to do for the next call? In that case, we'll send out an e-mail requesting, putting in writing, what kind of input might be helpful for the next call, and we can discuss that on the next call.

Anyone want to provide feedback on that idea? Okay. If not, this was another productive call. Thank you all for participating, and I look forward to speaking with everyone again the first Wednesday of May. Thanks.

STEVEN METALITZ: Thank you, Jamie.

[UNIDENTIFIED MALE]: Thank you.

[JAMIE HEDLUND]: Thanks, everyone.

[END OF TRANSCRIPTION]