Emily Taylor: I'm going to be on a plane this evening, and I'm not going to miss that plane.

Kathy Kleiman: So what's our deadline?

Emily Taylor: Our deadline, our absolute drop-dead deadline is seven o'clock, which is the point when I will be leaving; in fact it's quarter to seven to give me time to get to the front desk. I'm hoping to finish at six, so that we can all have a goodbye drink before that. So we'll do the carrot and stick approach. If we can finish – yes, I turn into a pumpkin before seven as you know. So if we ain't finished at six, I think that that gives us a good chance to slug this lot out. Let's review where we are at half passed five, Susan.

Susan Kawaguchi: Maggie just asked me to deliver one more point.

[background conversation]

Susan Kawaguchi: So actually one of the recommendations we had made to them when we were down there was to do some public outreach events, and we have a scheduled date of November 10th, and so they'll be coming to Facebook or to Palo Alto in general. I don't know if

we've decided on the location, it was either the office or our office, one of the two. And I'll be rounding up a bunch of brand owners, people that use the WHOIS record and they'll be delivering their message there. So they've already started on some of the recommendations we're doing. It's part of that communication thing.

Emily Taylor: Thank you very much. Yes, that's great.

Susan Kawaguchi: Congratulations to the compliance team it sounds like they're already starting on a number of your recommendations.

Emily Taylor: Yes.

Susan Kawaguchi: I still think you should take credit for them, but pushing in the right direction, but congratulations, you know that's –

Emily Taylor: It is, it seems like good work. Now, we're doing hard focus this afternoon, let's just recap and work out where we are. We let Marina Del Ray with a set of recommendations which were almost agreed. They fall pretty much under two headings, privacy proxy and accuracy. So far in Dakar, we have brainstormed some overall

categories to fit our recommendations under and we've made some progress on some of them particularly a sort of head-line data accuracy recommendation.

I propose that this afternoon as we are reaching the end of our time together, we focus on text-based recommendations and I'm looking forward to hearing how Kathy and Bill got on with their overnight task –

Kathy Kleiman: Terrible.

Emily Taylor: Let's get the text up there, let's please keep our comments crisp and to the point, and also focused on moving us forward towards consensus. That's how we're going to get through. And so with that I would like to hand over please to Kathy and Bill to let us know how you got on with the task of drafting your findings and initial recommendations on proxy and privacy. Thank you.

Bill Smith: I have the master document. Alice I just sent it to you, if we could put it up, that would be good.

Kathy Kleiman: And just a note, there's one more – number four paragraph, 42, the penalties, Bill, so I'll be circulating that.

Bill Smith: Okay.

Kathy Kleiman: But I just want to let you know, we wanted to put ketchup over our faces and come in and you say we duked it out.

Bill Smith: But we didn't – we didn't have time.

Kathy Kleiman: That's right.

Bill Smith: But Peter joined us as well.

Kathy Kleiman: Yes, that was great for a long time.

Bill Smith: Yes. This was done largely either in the restaurant here or out at the pool.

Emily Taylor: So you suffered.

Bill Smith: We suffered, yes. Alice is logging in now. So I'll start reading this, basically we – a lot of what we discussed were the things that we agreed on, start at those areas, and then went to the things where we might not have agreement.

So these are just bullet items, it isn't lots of text, but starting out, the community has not handled the issue of privacy in a timely or effective manner, that's how I just changed that so that –

Kathy Kleiman: Right, this is kind of findings before we get to the conclusions findings.

Bill Smith: As the community doddled, a private industry arose offering proxy and privacy services. The industry is largely unregulated, law enforcement and private industry around law enforcement have a difficult time finding those responsible for websites, and those are private industry around law enforcement is a language Kathy came up with, which is descriptive and if that's acceptable we use it, but it indicates that these are not just – it isn't just for law enforcement, there are others that are helping with cyber-security, cybercrime, et cetera that may need access to this information.

Data protection –

Emily Taylor: Sorry to stop you, Bill, Alice would you mind increasing the font size for those of us who are aged.

Kathy Kleiman: Just a note to Alice; one more paragraph about to come over that can be added to the document if you would. Is that okay, Bill?

Bill Smith: Um-hmm, ooh, that's big [laughter] –

Kathy Kleiman: If it doesn't say it, can we add the word "findings" at the top?

Bill Smith: It doesn't but yes I'll –

Kathy Kleiman: Alice, could you add the word "findings"? Is that okay Bill, we'll just kind of – because we're creating the master document.

Bill Smith: Absolutely. I didn't have time to – I'm not that old.

Seth Reiss: You were going to go there.

Bill Smith: Okay.

Emily Taylor: So we got as far as data protection.

Bill Smith: So now data protection, another finding data protection, commission or communiqués have told ICANN that natural non-trading persons need privacy protection under EU and other national protection laws.

There are protection for free speech and freedom of expression that need to be taken into account. Proxy and privacy services meet a market demand. Proxy and privacy services are terms used in the 2009 RAA –

Kathy Kleiman: But we should add, "but are not defined".

Bill Smith: But are undefined.

Kathy Kleiman: Alice, could you add that in there, "but are undefined", right.

Bill Smith: Yes, some of these I didn't have a chance to clean up, I was typing as we were talking, but that –

Kathy Kleiman: Between fist fights.

Bill Smith: But are undefined.

Kathy Kleiman: Thanks for taking interruptions, Bill, I'll try to stop.

Bill Smith: There is a risk within the current privacy services regimen that the registrant could be seen as invalid on its face as inaccurate, because of the registrant name, the privacy has – because it is the registrant's name, but a privacy service contact information, so this was stuff we talked about yesterday, and now into conclusions.

One, drop proxy services from the RAA since the proxy, as an agent is in fact the registrant.

Two, proxy and privacy regimen is flawed, and we direct ICANN, the Board and GNSO, as appropriate to fix it.

Kathy Kleiman: And we could have stopped there, but we didn't.

Bill Smith: We didn't.

Kathy Kleiman: We've got some more detail on that.

Bill Smith: We got a little more detail.

Kathy Kleiman: Just a bit.

Bill Smith: So let's see, where was it, so ICANN must develop and manage an accreditation system for privacy services, and we would need to put a timeframe in. We didn't have time to come up with a recommendation.

Once the accreditation system is – and some of this language is stuff that was taken from the recommendations already. Once that system is operational, ICANN should take steps necessary to ensure that registrars and resellers cannot accept registrations from unaccredited privacy service – proxy – providers.

ICANN must establish clear and consistent rules also at the time frame for accreditation for these providers that must include – that WHOIS entries have a flag that this is a fact – is a private registration to distinguish it from – so that you know that while you may not be able to contact a named individual through this contact point, it is not an invalid registration.

Privacy service must provide full contact details for itself including name, address, phone, email and a 24/7 contact, we think we may get some push-back on that, but have said in essence there need to be SLAs around privacy services.

Standardized relay and wriggle processes and timeframes need to be defined, something – again not all this language has been flushed out.

There need to be rules for the appropriate level of publically available information on the registrant. There we meant whether it's – there should be name, but now are there other things that should be in that as well, Kathy.

Kathy Kleiman: I'll just add color commentary, that the ideas that the community as a whole should set a common level. We don't want on privacy service revealing X, Y and Z, and another – let's set a consistency of this, so that as part of this policy development process that will take place, establish a common set of rules on this.

Bill Smith: Okay. Maintenance of a dedicated abuse point of contact for the privacy service provider.

Privacy service provider shall conduct periodic due diligence checks on the registrant contact information. So potentially on the way in, but then on a regular basis, to make sure that it continues to be accurate, and then that there must be a balance between privacy

and security and here all I threw in is sort of the height of the bar, how hard it will be to disclose information, if that's very high, then security – right, there are other issues then around security that need to be brought in, and if the bar is very low, there is a balance and that this is not just a privacy issue, that there is where privacy and security overlap, and the community or the board, whoever is dealing with us, we're trying to give them a direction and say this needs to be factored in when you do this study.

Kathy Kleiman: And the top entity needs a law enforcement LE and security industry. Could we add the word "security"?

Bill Smith: If I could just finish, and then – a definition of proxy we just wanted to offer simple definitions for them.

A proxy is an agent for the registrant and all data is that of the agent and they assume all rights and responsibilities of the registrant, they are in fact the registrant.

Seth Reiss: So that's local –

Emily Taylor: Let's let Bill get through it, and then I'm going to take questions and comments.

Bill Smith: And for privacy the registrant's name and a subset of other information which could be the null set, so it's possible that nothing else is in the WHOIS record, but it should be consistent across ICANN.

And then there's the ICANN should develop a graduated and enforceable series of penalties for privacy service providers who violate the terms of their accreditation, and that's consistent back to what we're saying on the registrars and others to the RAA, that those agreements need to have graduated enforcement options for compliance.

Emily Taylor: Can I first of all say, thank you so much, Kathy, Bill, Peter for producing this work overnight. I think that this is constructive, it very much acknowledges and builds on the areas where we can agree and is positive in that regard. I look forward to the comments and refining the text. I can see that it's based quite closely on the previous draft, which we discussed together in Marina Del Ray, and I hope that the people participating remotely are able to see this and to take it in as well, and look forward to their comments as well.

So in my list I have Peter and Seth, does anybody – Wilfried, Lutz.

Peter Nettlefold: So obviously I was a bit involved in this so I'm not going to say too much. I just wanted to put – as Bill has pretty much just sort of read out what's there, I wanted to put a little bit of flesh behind the thinking, just so that there's some things which we discussed ourselves. So it might help if we fill you in on some of those discussions, just so that it doesn't look like where did this come from.

So one of the key points it sort of struck, which we tried to get a clear flow of the argument through the findings, before we got to the recommendations is that it seems to us in terms of how the community may respond to this, that's it – one thing we wanted to avoid the perception of this was that we're being overly harsh on privacy issues. And we don't see it like that. At the moment as the findings sort of lead the argument along, this is unregulated.

There is no policy there effectively, and something has sprung up, but despite all the problems that that has created and people have told us in our submissions, it seems to fill a market need. It seems from letters that come from data commissions and so on, that's a legitimate need, and even if we didn't have those letters, then we can pretty imagine some cases ourselves where there may be a legitimate need.

So it seemed like what we're in fact doing is legitimizing this practice for the first time. At the moment, on the face of it, stuff which uses privacy service is inaccurate data and we're in fact putting a framework around that says no, that's not in fact the case, we're legitimizing it.

So then the next step is how do we do that in a sensible way that it doesn't make this Wild West? And what we wanted to do was as Kathy pointed out with the comment that we could have stopped there, is put a framework around it. We are aware of the tension that we don't want to be developing policy, but at the same time we don't want to say, after all this work, develop a policy, because the community has clearly struggled with that.

So we're providing – I don't think we are developing policy, I think what we're providing is a framework for developing the policy. The policy should look at how this – they should look at how it's accredited, they should look at what data should or should not be in. Like if it's limiting data, what data should be limited and so on.

So we're pointing to the things which need to be in a policy, or that should be considered in developing a policy, a key one being, that we need to balance the need for privacy, versus the need of law enforcement, security, the stability of the internet and so on. That's going to be a tricky one. But we're providing a framework for that to happen, and as Bill said, one of the things depends on exactly what information is in and out, it would seem to me, and the threshold for releasing that information. They're going to be key things for the community to decide in developing a policy.

So if the information is going to be given out very easily, you know if there is just a need, if someone wants to know essentially there isn't just an automated data troll, then we may – that will be one point where the balance is reached. Whereas if the threshold is

very high for the release of data, you know clear evidence of actionable – whatever the wording is, you guys – people who deal with this on a day to day basis are much better at it than me, then we will need to balance that in other ways.

So there's going to be a balance depending on where the threshold for what data is in and out is limited in the first place, and where is the threshold for releasing that data. We haven't recommended anything there that seems that that's something which would be duked out in the policy process between the law enforcement people, the data protection people and whoever else has an interest in this. But we have suggested – we've pointed to that, because in the policy development – in the development of the policy, that's the key issue for them to focus on. We don't want that to be missed.

So we've pointed at things that really for common sense reasons should be in, and we've pointed to where we think there is a key tension that they're going to have to focus on. So I'm sorry for stealing the mike, but that's kind of the thinking I think that was behind all of this, so I hope that helps.

Emily Taylor: Thank you very much, Peter, that does help and it may be worth just – it might be that I missed it, but the putting into words this idea that this is a framework for creation of policy, rather than you know so Seth?

Seth Reiss: So basically Emily said what I was going to say. I'm personally grateful to the three of you, because I think when we are able to reach a consensus on these difficult topics, it makes our team able to make a more valuable contribution, so I'm very impressed, thank you.

The other thing is I'm worried about that one definition. Alice, can you put it back up?

Alice Jansen: Which one?

Seth Reiss: Because I think using the word "registrant" like that is part of the problem, and if we could get rid of the word "registrant" in the proxy definition, and I'm not sure how to do that, but I think that's something we should strive for, because I think it confuses the issue.

Emily Taylor: Right, let's just run through the initial comments from people, notes that – I note Kathy that you want to come in on that. But let's have people think about this as well. So I've got Wilfried and Lutz waiting, and then I'll come to you Kathy, thank you.

Kathy Kleiman: No, no, you're right –

Wilfried Woeber: Yes, first of all, thanks to everyone who was involved in putting this text together, I like it very much. The only question I'd like to ask and that's not sort of suggesting, just asking the question that we do this consciously; I have the feeling that the user must – in the very beginning of this proposed text might actually sort of step across the boundary of our mandate.

In particular, after listening to Peter here saying that we are creating a policy framework, by putting this text together. I'm fine with doing it, so I'm not arguing against it, I just want to ask the question to everyone around this table, is this actually what we want to do consciously? Personally, I would rather use the wording like we mandate, or we suggest, or we advise ICANN to do this, but then again, we might sort undermine the – yes, we might break sort of the edge of the whole thing.

So as I said, in principle I'm fine, but if and when we do that, we should do it consciously and maybe sort of even add a little bit of an explanation towards the end of the document, why we think we've got the right and the mandate to do as we are doing.

Emily Taylor: Thank you very much Wilfried. Good points from both of you. Lutz?

Lutz Donnerhacke: First of all, thank you for your work. I'm really impressed how far you are going into details what the framework should contain. What I miss in this – just caution here is which part of the WHOIS entries might be considered to be covered by a privacy service?

We're talking about the registrant, but the registrant has a lot of entries, has technical entry, technical contact, has the billing contact, all mentioned in there you see. So we are talking about privacy service, or privacy – or registrant data, I should have to make the command that we should limit it to the registrant records for WHOIS registrant itself, the owner, and might be administrative contact, these are both critical contact details for the privacy issues.

If we're talking about stability and security, we need direct shortcut access to the technical and zone contact. That's the same way the ccTLDs in Europe usually implement it, if you are making WHOIS ccTLD, you get technical and zone contact, nothing more. For everything else you have to make a more complicated pause. So the first question here is how far can a privacy service go into these details? If you do not define it might be such a service even goes to the technical product, preventing the access or showing up the names of the server domain. I don't think so.

Second part. If you are going the who will – the recommendation for the framework, insists on accredited services. I don't think – it would be nice if you have every privacy service who is in direct contact with ICANN, it would be fine. But I don't think it's achievable. Privacy service are mainly in work due to applicable

local law, so they have in first place to fool with the local law and it might be a protection, in most cases it will be a violation of local law, to have another contract which starts then to provide more information than they allow to the local law.

In order to prevent this conflict in the first place, I'd like to rephrase it to there have to be a contractual relationship to an ICANN accredited entity, might be a registrant country, so this might be possible to construct a privacy service within the – within a country only following local law, and only have contracts following in the local law.

Emily Taylor: I've got Susan, and then I'm going to come to you three for any comments on that sort of – so what are we doing at the moment is just getting initial reactions and then I'd like the three of you to figure out how you'll get to respond please.

Susan Kawaguchi: So just more housekeeping, is it possible that we could get this document sent to each of us, sort of quickly, because it's hard to read it in full the way it is, and then – and it may be in this and I just missed it, but did you give any thought to grandfathering or you know what happens to the old bad data, you know going forward?

I think we should be explicit about that and I'm just wondering if this going to be perceived as harsh to the privacy services, as you

brought that point up, and sort of letting the proxy off the hook. Because yes, they're going to be responsible proxies are the registrant and ICANN is not letting them off the hook if all of the details are removed from the RAA. But the only – then ICANN has no ability to come down on bad proxy services, and the only outlet will be, I'm not talking very well today, so I'm sorry. But the only way to resolve an issue with proxy service then is going to be the courts. And I just wonder if the community at large is going to wonder we came so hard on privacy. I mean we could all state that argument, but I still think that's going to be a consideration.

Emily Taylor: Thank you can –

Seth Reiss: …proxy services that won't be addressed by this.

Susan Kawaguchi: Because we still won't be able – if there was a proxy service, then it is for right now, and let's just take ABC Proxy Service, right they are the owner, they are the registrant of that domain. So therefore they technically should be liable, but if you really are doing an enforcement action of some sort, you would need to get behind that information and get to the person that could actually take down that information, or change that. So yes, you could sue, you could list them in the complaint, in the litigation, you could file a UDRP, there's a lot of things you could do, but there's not

going to be any quick method for giving some sort of quick result mechanism for the privacy, but now we're not addressing the proxy. I just think it's going to be an argument the people will bring up.

Emily Taylor: I think those are all points well-made and I think my impression is that on the market out there, that proxy services tend to be more popular than privacy services. I don't know if that's completely based on no evidence whatsoever.

So Kathy, Peter, Bill, can I ask you for your responses?

Kathy Kleiman: I'll try a few.

Bill Smith: Just one, a very quick thing to Wilfried's point, we chose "must", I'm happy to back off of that. What we basically said was, we feel we need to give direction to the community, and it needs to be in as stronger terms – basically as strongly as we can make it. What is the strongest we could say, we could back off that, but we want to make it clear that it's not enough to say, yes, we're going to take care of it at some point in time, it's like you have to do something here.

Emily Taylor: Thank you, I'll go to Kathy, Peter and then I have you Seth.

Kathy Kleiman: Okay, let me just run down a few of the questions. First, we're working with a draft, so under definitions, pick your definition, the goal here is to have a definition of proxy, and privacy services; not for ongoing contracts, but based on our understanding of the community, this is what we understand privacy to be, this is what we understand proxy to be. So privacy is where at least the registrant is listed. So these are kind of and maybe we can even call that working definitions, but feel free to change the wording.

I had a note also about the "must" that "must" should – the idea is do something, or as Bill would say, fix it.

How far can a privacy service go in terms of what they have to reveal and what it shouldn't – we decided not to go that far, that if we're directing the privacy of a policy development process to start, let's leave it with as many of the policy questions as they can answer, we're just trying to create a minimal framework, and even for that we will criticized guys. So this is a minimal framework, let's leave the detailed questions to the community, because that's where it belongs. In terms of the old bad data, is that a question we can frame for the community to answer? And if so, let's add it in as a bullet point.

And then I made – let someone else answer the rest of Susan's question.

Emily Taylor: Nicely done. Well, as for Kathy, it's like Oscar Wilde says, "There's only one thing worse than people talking about you, it's people not talking about you."

Peter Nettlefold: I love going through it, because lots of stuff's already been said, thanks. So just to go look to where I'll start, I think there's still some outstanding issues. So in terms of, and I agree with Kathy, we deliberately stayed from what data should and shouldn't be included but I also take your point which I think is really important in that we're looking for privacy services to offer a service that the people need or want and in terms of the balance of that, we've – what is needed for security and stability if technical and zone contacts are absolutely required for security and stability reasons, and they're not really required for the privacy of the registrant owner, I actually think we should say that, so that there's a line in the sand. So these people need to be known for security and stability internet.

The rest of the stuff, the community can decide where to put the scale based on, and I think in terms of what you were saying about whether it's mandatory because of local, national laws; I think we can fix that potentially at the same time. And I'm sorry that I missed this myself being the government rep I should be very interested [laughter] in the local laws. But let's say again let's give the guidance to the community. So the community decides where to draw the boundary consistent with relevance national laws – or applicable laws. So we just put it in there. So when the

community goes out and has the bonfire about what data is in and out, it needs to be consistent with national laws. Would that take care it at that point?

Lutz Donnerhacke: I'm astonished about you, usually –

Peter Nettlefold: You're astonished or embarrassed?

Lutz Donnerhacke: I expected that you are saying the policy for privacy service which falls under local law has nothing to do with ICANN, because rom the GAC the point of view, it's national law, and national law has nothing to do – be regulated by a company, a private company in a foreign country, it doesn't have any influence to our local law, so I'm really astonished that you're accepting from – I thank you for the GAC, I know it's not true, but I thank you for the GAC here, and I take the good feeling was made that GAC is accepting ICANN to making policy even if they are conflicting just the law in various countries thanks.

Peter Nettlefold: I'm not sure I did say that, if it's got to made consistent with – it has to be made consistent with national laws, so it's not that –

Lutz Donnerhacke: But on the other hand, you know that there is no consistent local law at all.

Peter Nettlefold: Indeed. So this is something that would need to be discussed if it's the lowest or highest common denominator type question, yes. So but don't quote me that I'm saying consistent with local – but yes, I think we deal with it at that stage. And whether that ultimately precludes complete universality then that's I guess a question that in the policy-development process, but if we have it inconsistent with national law, we're not going to be allowing the policy to breech any national laws.

However that needs to be achieved by raising or lowering about to – you know raising about the bar to the highest standard which I think is the laws probably or a lot of the national jurisdictions are coming close to that and taking that on board, or whether we allow some variability based on different national laws. But that's something that can be dealt at the time. So long as the law aren't breached.

Seth Reiss: Good luck.

Peter Nettlefold: Thank you. That's why we're not resolving that here ourselves, we're passing that one on.

So you're grandfathering positioning as Kathy said, we actually did have a quick chat about this and we – I guess it's kind of assumed that's a detailed implementation question to do with grandfathering existing blah, blah, blah; and transitioning, happy to make a note about it, if you think it's helpful.

Kathy Kleiman: I definitely think it's helpful.

Peter Nettlefold: Okay, excellent. And your last one, our proxy is off the hook, that's a great question and I think I actually mentioned this to you in Marina Del Ray when I first put this forward, I would love your views; you, Bill, Kathy, people who deal with this. I guess we're trying to imagine what the situation is, if there is no mention of proxies. So proxies as such don't exist.

And so say you're the proxy service provider or the agent and you're assuming a bunch of responsibility and risk associated with that, and in the best case scenario nothing ever happens, because the person that you've assumed that risk and responsibility for doesn't do anything wrong, that's great.

Now, if they do something wrong, there's different sorts of wrong, if it goes to the courts, then it probably doesn't make much difference one way or the other, it's the in between categories where people are relying on good faith or things which you know don't have the force of the law behind them.

And I'm genuinely interested in whether you think this is a retrograde or a positive step. Do you, as the agent, get called out for it, and so does it make it clearer or less clearer, I'm really genuinely interested. Because if you think it's a bad step, I'd be entirely – I think it wouldn't be – it's good from my point of view, but I'm happy to be wrong. And if it's better to extend accreditation and policy and a framework around proxies then I'm happy to go there.

I think it will be difficult and you know we'll need to acknowledge that it won't be as transparent, because we won't know who the proxies are all the time. But if you think that's better, I'm happy to go there, I'm genuinely interested. My goal is to clear up the myths and make it better.

Emily Taylor: Well, let's make that note and the suggestion, I've got Seth and Wilfried on my list, does anybody want the mike as well, because then what I'm going to do is take these two comments and if I may, I'd like to suggest that the three of you produce the next draft, take some time to produce the next draft, taking on board the comments.

If you don't feel like you've got enough from us, then we can certainly do a bit more socialization, but I think probably – you know there's some obvious amendments that you yourselves have suggested, if we took half an hour at this stage with that amount, I don't want to kill you, I think that you've all been working very

hard, what's going to be the way of advancing our agenda this afternoon and getting an agreement? What are we thinking about that? Seth and then Wilfried please.

Seth Reiss: I think this relates a little bit to that further discussion. You know Susan what you said confuses me. Alice did you get my email by any chance, can you throw that up on the screen.

I guess I'm seeing this proxy differently, and I don't know if you were just talking about grandfathering but I see it as the proxy is going to list their own administrative contact, and if something needs to change, they would have the ability to do that. In other words, you wouldn't have to go behind anybody, and you're smiling, so you don't think that's –

[background conversation]

Seth Reiss: No, but I mean you need to tell me since you have the street experience you need to tell me what about my thinking is wrong. And maybe it's not wrong, maybe it's because that's not what, how it's happening now, but if we send a clear message that what's happening now shouldn't be happening, then the new proxy services, which I don't see as being accredited, but maybe they will be, just couldn't function the way they are now, because it would be too much liability attached to it.

So this is my attempt at doing a definition that doesn't create a double meaning for the word registrant and I don't know if this helps and I'm not suggesting we accept this, except that it clarifies things in my mind. So it's maybe a point of discussion.

And as far as the "must" I was thinking "should" might a good word, but that's up to you and I am available if you need my help.

Wilfried Woeber: Yes, actually the text which is on the screen already takes three-quarters of what I would have wanted to suggest and – sorry, my apologies.

In the previous version, like the three person proposal, I would have suggested to replace for the proxy thing the word "registrant" with the term "the user of the domain", because this is – not in this one, the previous one, yeah, the original one. But I'm more happy to use that one, because it makes it much clearer that the proxy agent is actually the registrant, and thus completely fits inside the system of terms and the systems of regulations and procedures.

Emily Taylor: Thank you very much both of you. Peter, you wanted to make a comment?

Peter Nettlefold: Yes, it's really on the next step. I again defer to Susan with Seth's new definition. Anyway, so Seth's definition if there is a residual

concern about this proxy approach, what I was going to propose is that the three of us who drafted it and you potentially step outside and have a quick chat. This is where the ketchup might come in.

No, no, no, go and sort it out and while the remaining members pick the next tricky thing and start to come up with some text, and then we can come in and look at your text, and that we've got two jobs going at the same time, that's all I was going to propose.

Emily Taylor: I think that that's – I would endorse that and perhaps those of us remaining in the room can revisit the accuracy recommendations that we were starting to work through yesterday, and see how we're doing on that. Or if there's another tricky subject that you want us to work on, we can.

How about we all take 15 minutes anyway and have a break and then come back in with our revised text at four o'clock, yeah?

[background conversation]

Emily Taylor: Have like a break and then work on it, half passed three? How long will it take? Half passed three.

Susan Kawaguchi: This is Susan, so I think everybody, when we're looking at the proxy issue, we should keep this in mind; 2009 RAA addressed the proxy issues. We haven't seen improvement since it was addressed. 2001 RAA did not address it at all. If you search it, there's nothing about proxy in there.

So we've had a lot of bad behavior going on in the proxy realm without that – the language of the 2009 RAA and the language of the 2009 RAA was trying to fix the proxy issues. So litigation, whatever UDRP process, whatever was not able to deal with the proxy issue, and then there was some quick fix, put into the 2009 RAA.

But basically, what we're doing is reverting back to an existing situation that was not good, if anybody has looked at proxies, you'll know that it was not a good situation. And so what are we going to say to that community that says no, we fought hard to get this put in the 2009 RAA and you're stripping it out. And if there's another one in between, forgive my ignorance, but we need to look at all the RAAs.

Emily Taylor: So why don't we take a break now, then so the small groups. You want to –

Wilfried Woeber: I do see your point, but at the same time we have to recognize that this attempt failed miserably, so I wouldn't have any bad feelings

in suggesting to rip it out again, because it didn't work. I mean it was put in but it didn't get us where we wanted to get to, so yes.

Emily Taylor: Seth.

Seth Reiss: Yes, I guess my feeling is if we, as a team, give this definition, we're sending a message that the old, old RAA doesn't mean what people took it to mean, that they're free have improper proxies. So I think it's very important that we send this message that clarifies what a proxy is to us.

I don't know – I know you still have concerns, but I think it's a matter of telling the industry that they're on the hook, if they continue to do this. And I don't know if we need ICANN to say that in an RAA, because your previous suggestion was just to take off that language, but that is kind of acknowledging that you can be a registrant and not be a registrant. And I don't think that's true. But so anyway –

Emily Taylor: Okay.

Susan Kawaguchi: I just want to make sure that we really think about what we're doing.

Seth Reiss: Yes.

Emily Taylor: All right, let's take a break, come back into the main session together or sort of all get back together at sort of twenty to four, see how we've got; does that leave enough time to process a new draft, or would you like until four o'clock?

[background conversation]

Emily Taylor: In that case, let's work through – let's take a break and then work through the draft on the screen together, that's probably the best thing to do, because I sense that everybody's interested and everybody's fairly close to being happy with it. We've got a big issue to work out about the extent to which proxies are included in the framework which you have described and what will be the most effective way of getting change I think.

Bill Smith: I think the intent we had in the framework or the direction is that around proxies is that they actually have to act responsibly. I don't know how we can put that into an ICANN contract, but it's basically if they're served with process, they have to respond, and if they don't then ICANN should have procedures in place where

registrants who refuse to participate in processes or whatever, they dealt with, you know enough of the games.

That's the message we need to deliver to the community is you can't hide behind people for the real reasons, that for privacy reasons that are legitimate. But the games people have been playing are no longer acceptable in this industry.

Peter Nettlefold: Yes, so again this comes to sort of genuine questions rather than my opinions, so in terms of what I had understood, like I think Seth said it really well, so 2001 and 2009 RAAs, we know it hasn't been good, so that's clearly what we're trying to fix. And so pulling out language I can see how this will be perceived, and this is why I'm really, like I'm really interested in this. If I get this wrong, yes, it won't be great for me.

So putting in a definition that clarifies or doing something in our report that makes it crystal clear, like I'm interested in whether we need to do more or where the residual problem might be, if we say, you're the registrant, in our proxy you're the registrant, and so if there's a problem in the fact that they don't respond, that should be the same problem that we would face with any registrant, I would think. Or if there is any problem that is associated with that registration, it should be the same as the problem with any registration and do we have the tools in place to deal with that for other registrants, then we should focus on that I think.

Kathy Kleiman: We have a responsibility to respond.

Peter Nettlefold: And so –

Kathy Kleiman: And if the main registrant, I get emails all day long, I don't have a responsibility to respond to those.

Peter Nettlefold: So is that where the problem is? And so let's focus on that. So if we fix this up, maybe we've been looking at – I thought this the other day and I wasn't sure you know whether it needed to come up, because I remember a couple of meetings go, Bill first I think articulated what we had all been thinking about service level agreements because I remember it popping on as our recommendations and I think we all agreed that when it was on the table… And as I was drafting these GAC analyses, I wondered what it means.

And when I drafted the text, I in the back of my head, just because I was reading so many of the submissions and people said relay, review, process; relay, review, process; times for relaying and reviewing, blahdy, blahdy, blah, I thought that's what it means, that's the way I drafted the text. It seems to me that maybe I missed the broader problem.

In fact for proxies, we're not worried about relay and review, because you're the person that's in trouble. I don't care if you relay and review, it's you, you're the registrant. The problem is to what the SLA issue is how quickly you respond and how you respond, and that's the same for every registrant potentially. So I'm just putting this out, I'm not sure but are we looking at a broader problem and potentially we need to focus our attention on some recommendations on the broader problem.

Kathy Kleiman: So and I don't know how –

Emily Taylor: Let's have a break, come back in ten minutes.

Kathy Kleiman: It's hard to get ideas out when, I mean I agree with the break, for one thing I have to go to the bathroom, but it is really hard to get ideas out and I'm worried about Sarmad's opinion here, because yesterday he was very adamant that a privacy registration was false WHOIS information. So that's what I understood.

Emily Taylor: That's reflected in the text here.

Seth Reiss: Currently it is.

Susan Kawaguchi: So I haven't had time to really absorb this document, so –

Kathy Kleiman: We have a duty to respond, just wanted to note what Susan said that her inbox is filled all day long, and so if I get a thousand offers a day from my domain name, do I have a duty to respond to all of them?

The answer is almost invariably no, but a note that in – that from what I've been told from my communities, having your information out there, particularly your email out there and all available, all accessible all the time creates spam. So that one way to make sure that the messages of cyber security people and law enforcement go through more quickly that people are doing is privacy services so that it's really the important stuff that comes through.

So before we change duties to respond to things just noting that maybe what we're talking about is how the really important stuff gets through, and then there's some kind of duty to respond to law enforcement, or to cyber security people and I don't know how we get into that detail, but we are at the point of passing a lot of these details onto the next group.

Emily Taylor: I think that's – let's have a break, back at quarter passed, is that too long?

Seth Reiss: Quarter passed.

Bill Smith: Quarter passed.

Emily Taylor: And then come back together and work –

[break]

Emily Taylor: Okay, settle down everyone. Alright, we've used this time to sort of talk informally and circulate ideas about this draft. Let's get this new draft up on the screen. What we're going to do is, first of all, any show stoppers please in this whole thing? Okay. Well let's go through it slowly line by line then.

Kathy Kleiman: Point of information – James has many conflicts throughout the day and is also trying to see a doctor, so I'll just share that. it's a good question to ask him also, is there anything exploding here. It seems to me we're trying to…

Emily Taylor: Has he got a copy of the text via email?

Kathy Kleiman: It would seem so. Everybody's got one.

Emily Taylor: I would send our best wishes to James and if he can find the time at some point this afternoon to scan through and give us any immediate show stoppers on it, we will continue in his absence.

Kathy Kleiman: Would it be possible to send him the most recent version? Dr. Sarmad has added some technical contact language under both "findings" and "conclusions", which we'll get to at some point.

Emily Taylor: Okay, let's get the most recent version up on the screen please.

Female: For remote participants, we're still here, just no one is talking. Thank you.

Emily Taylor: We're just waiting for the – ahhhh, there we go. Sarmad, please talk us through the latest additions and then let's go through the text together.

Sarmad Hussain: So this is just following Lutz's earlier comment – there are three different sections of information, and I guess the question to ask is, the technical contact information, is that relevant for privacy. And if it's not relevant for privacy, it is definitely very relevant for the operational issues and just security kid of issues. And if that can be excluded from the privacy debate so that the operational issues and security issues are not undermined in this process…so a couple of simple sentences added, one in the "findings", which says that technical contact information has special relevance and use for operations and security community.

And then if you scroll down, somewhere in the "findings", added a statement which says that after consultation with the community ICANN made a quiet publication of its current technical contact for operational and security reasons. So I'm not sure whether this is articulated very clearly, but what it's saying is that the technical contact information that part of the information is not, cannot be private and should actually be just given out.

And that's probably what Lutz was alluding to as well. Is that something you were also suggesting or is this different from…

Emily Taylor: Okay. Are there more changes for you to take us to Sarmad? Thank you very much for that. Wilfried.

Wilfried Woeber: Following up on the private discussions we had during the break – I fully agree with the goal, the comment is only regarding the user of words because to be precise we don't want to have technical contents of a registrant, we want to have a technical content for the DNS service for that domain. Is that correct Lutz? Because sort of, the registrant is usually a human being or an organization.

Lutz Donnerhacke: That's not quite correct. We have two contacts usually. We have a zone contact what is responsible for working DNS and we have a technical contact which is responsible for everything wanting technical behind these domain names. That's quite different. If I have a name server for instance, if I have a problem with the zone contact because it's responding with incorrect data pointing to another zone which is not allowed to point too or something like this. Then I have to go to the zone contact.

The technical contact is the person I have to call if I have a problem with the mail server or something like this. The service provider using the domain name, not the service providing the domain name itself. Zone contact is for the domain name itself and technical contact is for all technical issues which use the domain name for something.

Emily Taylor: Sorry to cut across you. I think that if, is your wordsmithing…you're content. Susan.

Kathy Kleiman: I think this is an important inclusion, especially coming from SSAC, that I can see certain privacy reasons why – somebody may have a server in their own house, they may be their own technical contact. However, in general, it's my sense from my community, from various communities that I participate in that the technical contact is generally not necessarily the registrant or the administrative contact and it may rise to a higher level of disclosure; higher reasons for disclosure.

So I think this is interesting, and notice, we're still saying "after consultation with the community". We're pulling this particular field out as one that may – this whole privacy framework is about, this privacy/policy minimalist framework is all about balancing the needs of law enforcement and security community with the needs of registrants. And we're highlighting this one field as having a slightly different balance and we want to point that out to everybody.

Emily Taylor: Okay. Let's go through from the start of the document please.

Susan Kawaguchi: This is Susan. I'm aligned with your concern there and probably most of the time it is not going to be a registrant that is controlling their own servers. But I am concerned that a technical contact on a registration has some control over that registration, they control the

servers. Because you can, if I am just the technical contact, not all registrars would follow this, but I could contact a registrar and say I am the technical contact. I am not the admin contact. And I can change servers on this.

So we may be forcing people by having that true technical contact information revealed to actually have two levels of a privacy – they may be contracting to someone else just to be a technical contact so they don't have to be divulged there.

Emily Taylor: Guys, interesting though this is, I need to leave in two hours and twenty minutes. So my priority is to nut out these recommendations. If we don't make significant progress on the recommendations be the end of this meeting we are in serious problems. So I think we've made fantastic progress today, please let's keep focused here. There's lots of interesting stuff to talk about. I do not think that technical contacts are the most contentious area of this particular recommendation. Let's focus on the areas of our difficulties. We can wordsmith the issues relating to technical contacts in the course of time if that's okay.

So, what I'd like to do is jut to read out each paragraph and take your comments on each paragraph. If you have no comments please do not raise your hand. "Findings – the community has not handled the issue of privacy in a timely or effective manner." "As the community dawdled a private industry arose proxy and privacy services." I thought that was Bill definitely. Very nice.

"The industry is largely unregulated." Okay. "Law enforcement and private industry…" Why are we saying largely? "Law enforcement and the private industry around law enforcement have a difficult time finding those responsible for websites." Lutz, thank you.

Lutz Donnerhacke: I do not see the reason for the sentence. I do not even believe that it is true.

Sarmad Hussain: I think we have been told more than once that this is a fact. So I don't want to go into that discussion. My comment about it is that the wording here is narrowing the security activities to private industry and law – where is it – "law enforcement and private industry around law enforcement". There is lots of security relevant entities which do not qualify as private industry around law enforcement.

Kathy Kleiman: What would you call it? Private what? We're trying to say law enforcement is public maybe, private…

Sarmad Hussain: No, I'm thinking, just as examples I'm thinking along the lines for example of National Security teams which might happen to be just

a private limited liability company operating under the mandate of the government. I'm worried about…

Kathy Kleiman: So come up with a word, come up with words.

Sarmad Hussain: I'll try. Should we continue and I'll try to come up with something? That's better.

Emily Taylor: The major issue actually in this, or throughout, is whether we are intentionally limiting just to those who are doing a law enforcement thing, or whether we mean everybody.

Bill Smith: This is just a finding right? I think we may want to change the language but it basically is saying people have difficulty finding stuff.

Emily Taylor: …highlight the private industry, law enforcement for now and we'll come back to this. Yes please?

Kathy Kleiman: Is security in dispute? Susan, we were trying to think of an umbrella that fits you and Bill. What do you guys do?

Peter Nettlefold: I just have a comment. I think I have a counterpoint that I see no reason not to be very broad and I'll just point to the fact that we just did a consumer survey that says consumers have a tough time finding websites. So I'd really, maybe we just say users. It's a finding. We know users have a difficult time finding; users of WHOIS have a tough time finding people with websites.

Kathy Kleiman: Yeah I would agree with that.

Sarmad Hussain: We can also say "various stakeholders".

Emily Taylor: So, we've got suggestions of "users of WHOIS", "various stakeholders", Seth do you have a suggestion.

[background conversation]

Emily Taylor: Kathy.

Kathy Kleiman: After having been laughed at repeatedly for spending the last decade working on WHOIS, I would say it seem to me a finding of

this group that 10 years of studies, working groups and task forces is dawdling. It's not again, it's my characterization frankly of how this group has found my own work.

Seth Reiss: Yeah I agree with you. I guess I interpret it in a sense…

Emily Taylor: No, it's intentionally saying what it says and I think it's a fair point.

Seth Reiss: Yea okay.

Bill Smith: I'd be happy to change "dawdle", but the message is this community did nothing in terms of action for a long time, even though the EC over a period of years communicated "you need to do something".

Emily Taylor: Okay, well subject to those three different suggestions, let's move on to the next paragraph please. Unless, do you have a desperate comment to make Lutz?

Lutz Donnerhacke: I'm currently confused what the sentence…I thought it was law enforcement currently. Do you mean to say that it's changed the meaning three times in a very different way? Law enforcement people have completely other possibilities to find out what that website user is that normal users, end users of WHOIS is a completely different issue.

Emily Taylor: I suggest that we park this for now as it's not a crucial point, and revisit. I think the points you make are very valid Lutz. We would be saying three entirely different things according to which one of those we choose. Let's go through and revisit which of those three things we want to say. Okay. "Data protection commissioner communiqués have told ICANN that natural non-trading persons need privacy protection under EU and other national data protection laws." "There are protections for free speech…"

Sarmad Hussain: Just a question about why are we singling out EU in this context.

Emily Taylor: It's a statement of fact.

Bill Smith: We have several communications from, or ICANN does, from the EC on this topic, so it's fact.

Kathy Kleiman: Including an official opinion from the Article 29 Working Party, which is under the EU data protection directive, it's the National Data Protection Commissioners of Europe and this is their organization and it came from the Chair.

Sarmad Hussain: So if there was no communication would that somehow stop us from doing something like this?

Kathy Kleiman: A minimum not a maximum that this is one area for certain that we've been told – Bill and I were using the analogy "a floor, not a ceiling". At a minimum we've been told we have to protect these guys.

Sarmad Hussain: So could we word it so that it seems like an instance rather than a reason?

Emily Taylor: So could we propose for example, "ICANN's attention has been drawn to this situation for example, data protection commissioner blah, blah, blah, blah…" Yeah? The situation in previous paragraphs.

[background conversation]

Emily Taylor: To this situation or to this…

Kathy Kleiman: I think we're drawing the community – you know, "this is one of the things we found"…

Emily Taylor: Would that meet your concern? I know it's very valid.

Kathy Kleiman: Commissioner communiqués are one example and it sound like free speech protections might be a second example – two bullets underneath this line.

Emily Taylor: There are protections for free speech and freedom of expression that need to be taken into account, which is a very strong statement. "Privacy and proxy servers meet a market demand." "Privacy and proxy services are terms used in the 2009 RAA but are undefined." Sarmad.

Sarmad Hussain: Going back to a similar comment last time. Are we sure that they're undefined or should we say that we could not find definition of them?

Emily Taylor: I think we're sure they're undefined but.

Bill Smith: Yeah, in a search of the RAA, privacy and/or proxy servers occur and there is no, in the definitions section of RAA, there are no definitions.

Kathy Kleiman: And Bill showed it to me.

Emily Taylor: Okay. So we're satisfied that that is a correct statement? That's a very helpful comment. Thank you. Okay, next paragraph – "There is a risk that in the current privacy services regime that the registrants could be seen as invalid on its face as inaccurate. Registrant name privacy service contact info." Wilfried, thank you.

Wilfried Woeber: It's missing that the registration data could be seen as invalid.

Emily Taylor: Good. I think that's something that we don't even have to highlight thank you, that the….Alice, third line of that paragraph, delete "registrant" and make it "registration data". And I think we

probably just need to scan this for sense if we're comfortable with the meaning.

Peter Nettlefold: Again, just on timing, like I assume we're going to be happy to change single words or commas or things like that at a later date, in tract changes for each other and we just nut out the contentious stuff here. Because there's stuff here, I was involved with the drafting and there's some of it that I don't really like particular things, but I don't think any of the things I don't like change a substantial thing.

Emily Taylor: Okay. That's a very helpful. Let's try to really focus our comments on where it's going to affect the substantive meaning. So, we know what we're trying to say here and we have thumbs up. "Technical contact information has special relevance and useful operational and security community." I think, just if I may say, that's a nice broad encapsulation of technical contact information. It could be as little as name server and as much as the whole thing. Let's not have a big discussion guys on technical contact information. It is not contentious. So if you have a desperate comment you need to make Lutz please do, otherwise please hold it.

Conclusions – number one let's get – because these are our recommendations. One, so this is what we're asking ICANN to do

as a result. "Drop proxy services from the RAA since the proxy as agent is the registrant." We're comfortable? Bill. Lutz.

Bill Smith: Yeah I just want to make sure that we're comfortable with that since there was a fair amount of discussion on that topic before the break.

Emily Taylor: Yes. I have Lutz. I have Kathy.

Lutz Donnerhacke: Just reading from the RAA from registrant requirements, "customers may choose to register domain names through a proxy service where the proxy service is the registered domain name holder."

Kathy Kleiman: Which they can do whether or not we say so in the contract. I wanted to add that I was uncomfortable with this in Marina Del Ray and I think when we left, I know not everybody was there, but when we left I was the only one uncomfortable. And I actually went around and talked to registries and registrars about this and it's my sense that this is not going to make the community mentally happy, but that they understand that privacy and proxies have been talked about in the same breath and that it's time to

separate them out and treat them differently because they're different.

Peter Nettlefold: One thing we talked about in the break was potentially heading of I guess two things, community criticism and the potential for ambiguity that may arise from this by putting, at the same time that we drop the proxy services from the RAA, putting in an affirmative statement. To the extent that there may be a risk of confusion, I'd be pretty happy to see that I think. So that if we drop out the current word, and in fact what Lutz just read out was pretty good, but we could put it in, maybe we take out some of or leave bits, but we make sure that we ask ICANN to make sure that there is an affirmative statement of some kind in the RAA that clarifies that the person with the name in the registered name holder column is the registrant and blah, blah, blah; potentially what the words that Seth sent around.

So, to the extent that that would be a classic legal for avoidance of doubt type provision I'd be happy to see it in.

Emily Taylor: I've got a list which has Sarmad, Wilfried and Bill.

Sarmad Hussain: So just not recommending any wording, but suggesting that the wording be such that we say that we're not saying that this whole proxy industry should be closed down. We're saying that the

proxy industry could continue but with these new set of responsibilities. And the wording should articulate that a little I think more clearly.

Emily Taylor: Okay, I've asked Peter to see whether he can come up with a straw man sentence, do you have a suggestion.

Lutz Donnerhacke: Just for information I had put in the definitions I found on privacy and proxy servers in our RAA environment on the list.

Emily Taylor: So we're saying that it might be defined?

Lutz Donnerhacke: As a technical people I would say that it's not defined.

Emily Taylor: Okay, thank you. Wilfried.

Wilfried Woeber: Just for consistency, under item two I would like to add "at the moment proxy and privacy regime is", because I don't think we want to get the message around that also in the future we consider it as inappropriate.

Emily Taylor: Or yeah, "the current proxy/privacy regime" so we're talking about the regime and not the concept. Susan. I've asked for a draft to replace with this idea of affirmative statement. Bill.

Bill Smith: I don't think, the comment I wanted to make is I think there are other, probably other instances of proxy up on the ICANN sites and maybe other agreements and it's not enough to deal within just the RAA, we need to say basically remove it. And the point I was, why I was shaking my head was because in essence, at least as I understand it, we want to communicate to ICANN "get out of this business". Yes it exists, but it's something between the registrant and the agent and if you attempt to legislate here you're going to have problems.

Emily Taylor: Wilfried, you were on my list, but a long time ago. Sarmad?

Sarmad Hussain: So yes, I'm just saying that the part of the communities that we should actually articulate exactly what you are saying and not try to be concise here I think so that we don't enstrange them.

Emily Taylor: So, can we put a note on one for the moment to say "expand" and also "? Affirmative statement", which I think will remind us what we're talking about here? Yeah? And to capture your point

Sarmad it's more a question of the legal recognition rather than saying "abolish these services as services". It's more about what the service, what the implication of the service is.

Okay. "The current proxy and privacy regime is flawed and we direct ICANN, the Board and GNSO as appropriate to fix it." Sarmad.

Sarmad Hussain: Just a small thought, this should probably be before other recommendations. This should probably be a starting point.

Emily Taylor: You would prefer that as item one? Okay, does anybody object to Sarmad's suggestion that we move this as item one? Is that "No, I don't object" or "No, I disagree"? Okay. Thank goodness. Our first bullet point – "ICANN must develop and manage an accreditation for privacy services providers" timeframe. We know what that means. No? We don't like it? So, Lutz, you don't like the concept of having an accreditation system for privacy services? Okay.

Lutz Donnerhacke: The current situation is that it's free for the registrar to accept such a system and they have an obligation to have a contract for and what we are asking here for is to build a new industry and have an accreditation team in ICANN where the industry still exists and have completely other qualifications at the moment.

Emily Taylor: Okay. Does anybody want to respond to that? I've got Bill and Peter.

Bill Smith: My understanding of this was to actually not do away with the system but to regulate it. Currently it is an unregulated industry. And so as an example, using such a service, you may never – and we've heard this from law enforcement and others – you may never reach the registrant. You may never get any information. You may never get any response. No, that's not okay. Because registrants have an obligation to respond in other parts of the system, privacy services have no obligation to do anything and then nothing happens. So that is a significant issue.

Peter Nettlefold: Okay, I'm going to change what I was going to say because I just heard what Lutz said off the mic that it's okay that someone is never contacted. So I've really got to pitch this back to Lutz to be honest. In the findings you put your thumbs up when you said the systems broken, it's unregulated and it needs to be fixed. How do we fix it?

Lutz Donnerhacke: I had the understanding that the fix would be in extension with ICANN accredited registrars that if they make such, or allow such

contracts they have at least the following obligations to put in such contracts.

Peter Nettlefold: Okay, so that would be fine if it was only registrars offering these services, but it's not. So if we can say "ICANN accredited registrars can offer these services and here is the framework", and no one else can offer the services, I'm with you.

Lutz Donnerhacke: I don't have a problem with vertical integration. What I want to achieve here is that we have a recommendation and we have a framework in which privacy service operates. But I have a problem with every privacy service needs to be registered and have a special contract with ICANN itself. I do think it will cause a lot of more problems than we currently have.

Kathy Kleiman: I'm not sure that there's any specification here that the privacy service providers have to have a contract with ICANN. That may be something that flows out of the accreditation system, but it may be a contract like resellers, a contract with the registrar. But Lutz, what finally persuaded me was the quid pro quo that we're having somebody's name but the contact details, I don't want to say are false, but they're not the registrants. And that the quid pro quo for being allowed to do that is A – flag it, let people know, I'm not

really talking about putting up a new bite or a new field, but somehow identify that you're working through a privacy provider.

And B – kind of let the community come up with some standards, call it, we had all agreed on best practices, this is going one step past kind of a best practices recommendation to say let the community develop some standards for reveal and relay; that's the concept of accreditation system. If you want to come up with another word, that seems to be where we're going, but if we want to put in that it doesn't necessarily mean a contract with ICANN, I'd be okay with doing that.

Lutz Donnerhacke: That's okay. I have no problem with the framework, it's a common framework. I do have a problem with wordings that seem to be more than fulfilling its obligations. I have a different understanding of "accreditation".

Kathy Kleiman: What words would make you happy?

Lutz Donnerhacke: Instead of "accreditation system" I'd like to have something like "contractual framework" or "working requirements" or "behavioral requirements", "behavior framework".

Kathy Kleiman: Can we go with "working requirements" group?

Peter Nettlefold: I might go back to words that we already said we talked about. So, are we actually talking about best practice guidelines here and if they're mandatory?

Lutz Donnerhacke: Yes that would be fine.

Emily Taylor: Mandatory best practice guidelines.

Peter Nettlefold: Mandatory best practice guidelines.

Emily Taylor: This would fit into the sentence as "ICANN must develop and manage a" – delete "accreditation" – "a system of mandatory best practice guidelines for privacy services providers." Okay.

[background conversation]

Emily Taylor: Mandatory best practices. Okay is somebody – "system of" – let's have a look at it. Delete "accreditation" in the second line of – no, up in the previous bullet point. Delete – "a system of mandatory best practices…"

Wilfried Woeber: Non-native speaker – I think it's – what do you all call it, an oxymoron? You cannot have something which is best practice and thus being optional and at the same time being mandatory. That's my understanding of the English terms. I may easily be wrong.

Emily Taylor: Well, if it's causing that problem then the wording is, if it's causing that problem for us then we've got to think how others will read it too. So I think that's a point well made. Yes.

Kathy Kleiman: Can we go back to Lutz? Lutz, what would you…mandatory practices; a system of mandatory practices? Would that be okay? There we go.

Emily Taylor: You would normally say "requirements"; thumbs up?

Kathy Kleiman: What about keeping the word "must" folks?

Emily Taylor: Thank you. What would your proposal be?

Kathy Kleiman: I propose "must".

Emily Taylor: Propose "must" – are people comfortable with "must"? Peter.

Peter Nettlefold: Actually is everyone agreed on this? Maybe I won't say anything.

Emily Taylor: Alice, we've changed "practices" to "requirements".

Peter Nettlefold: I'm wondering if this gets mired in the sort of language that has baggage in the ICANN world, but are we talking about, maybe if we're not talking about contracts or guidelines, what about "code of conduct"? No, "mandatory code of conduct"?

Kathy Kleiman: "Mandatory requirements".

Peter Nettlefold: Because we're basically trying to say that you need to behave in a certain way whether it's in a contract or, it's written down…you're unhappy, okay.

Emily Taylor: I think requirements still there. "Once the accreditation system…", so, should we change that to "requirements" before we carry on? "The requirements are operational or" "the system is

operational; ICANN should take necessary steps to ensure that registrars and resellers cannot accept registrations from unaccredited privacy services providers." Okay, let's do concept first and then do the wordsmithing. So, objections to concept?

Wilfried Woeber: If we move from "must" to "should", which I can live with, we should really be consistent throughout the document.

Emily Taylor: Thank you, that's an important drafting point. I think that sort of we're going to have a tidy and a checking for language. Lutz.

Lutz Donnerhacke: The second paragraph coming up here is the reason why I had a hesitation again for accreditation. So, we're going to "requirements", "mandatory requirements", that doesn't mean that we have a system for it. I would rephrase the first thing to "develop management mandatory requirements with others systems", then the next one "Once the requirements are set up, ICANN should take the necessary steps to ensure that registrars and resellers cannot accept registrations from not behaving privacy…" or something like this.

Emily Taylor: I think that my immediate reaction on the language is that that will have the implication of making it a subjective test rather than an

objective test. In other words you go, as it's standing, we say "do you have the piece of paper"; "yes I've got it" or versus "how do I think you are behaving". So it's actually not just a wording change it really does radically alter the meaning, so bear that in mind. And I can see that Peter and Bill want to come in on that.

Peter Nettlefold: I'm going to try [Hakum's Razor]. Can we delete the whole dot point and go to the dot point above and say "ICANN should develop and manage a system of mandatory requirements for all privacy service providers."

Lutz Donnerhacke: And then we can drop the second point.

Emily Taylor: And then we chop the second point completely. Okay, so the bullet point Alice, beginning "Once the system is operational", which is below where we just are, the proposal is to delete it. I'm sorry Bill.

Bill Smith: I am beginning to have significant concerns about ICANN's ability to enforce any of this. I understand there may be language issues and that there in fact may be issues that some might have with privacy service providers having to execute contracts with ICANN. However, without a contractual relationship, ICANN can't do

anything. And that's the system we are in today and it has been demonstrated to not work.

The other concern I have is around, and I am comfortable with us moving to "should" instead of "must", however, having been in the technical community, "should" in the technical community as in the IETF, has a very specific meaning and it means that it is only recommended. And it means that there may exist valid reasons to ignore. Okay? And I don't think that's what we are intending here. I certainly and not intending it. I'm saying you guys, you may not do this, but if you don't do this you're putting the entire DNS in jeopardy.

Emily Taylor: Okay, that's a useful point to note. I've got Lutz; did you want to come in Seth? Did you want to come in Susan? No. So, Lutz and then Seth please.

Lutz Donnerhacke: The word "should" is here because we are making recommendations. For me it's the correct word. If you want to refer to the technical term in the IETF, if you want to use the word "should" in the sense that it is a must accept there is a valid reason to ignore it, then technical documents make an expletive statement how to use the word "should" in this sense. Otherwise, in the technical world of IETF, "should" means should as in the English language.

Emily Taylor: Thank you for that. Seth.

Seth Reiss: Yeah, it's interesting to hear what Bill said because me, the legal interpretation of "must" and "should" is if we said must we're overstepping the bounds of our scope. And we could be accused of making policy. But I understand what Bill said because I wasn't aware of that construction and so I guess we're a team of legal and technical people. So maybe we have to have a definitional….

But I thought the nice thing about this Bill, is that it doesn't say whether there has to be a contractual. It says what the end result has to be. And I think we have to be very careful to not do something because we don't think ICANN can pull it off. In other words, we need to make our recommendations and just because historically they may not have always pulled it off, we should be more optimistic that they're going to get it right this time.

Emily Taylor: Peter wants to come in so I'll go to Peter and then you Bill.

Peter Nettlefold: Yeah, look again, it's to follow up the point by Bill and then Seth and I have great sympathy with Bill's point. I guess the effect that we're after is that we're recommending that something must happen. If they take up the recommendation this has got to

happen. So they can forget the recommendation, but if they do they've got to have it. So the question is, is the word "accreditation" is the word "contract"?

Now, we all know if we have the word "contract", which we currently have in the RAA, it's not enforceable sometimes. So it's the effect we're after I think rather than the mechanism, to me; if it's an accreditation scheme or it's a contract or whatever. For me, and I'm not sure that mandatory is the right word, but mandatory seems really strong to me, and I could be wrong. Another word which I know that we've talked about, well I've put forward in some other way that I've drafted recommendations before was "enforceable". Now, I'd be happy to see that as an option. And maybe "enforceable" is it. And ICANN picks the mechanism, so they can still pick the mechanism; it's got to be enforceable. Maybe we do that.

Emily Taylor: Guys? So Bill are you comfortable with that? That's good and actually it sort of supports our theme when we don't know how to do something of just throwing it over the wall and saying "right, you do it." "A system of enforceable requirements" please. So the bullet point where we've got all the highlighting – "ICANN should develop and manage a system of" please delete "mandatory" and make that "enforceable requirements." Lutz.

Lutz Donnerhacke: Just to make clear, enforceable doesn't mean for me that it should be as strong as that. Not the least common set which seems to be possible to enforce over all. Okay, if we insist on "enforceable" we can direct ICANN to make a very weak set of requirements because everything else is not enforceable.

Kathy Kleiman: Can you live with this language?

Lutz Donnerhacke: Of course, I just want to help Bill.

Emily Taylor: Okay, so we had a proposal on the next bullet point, which is I think we're comfortable with this. We've got a thumbs up for that bullet point. So the proposal now is to delete the following paragraph – "Once the system is operational ICANN should take necessary steps that registrars and resellers cannot accept registrations from unaccredited privacy service providers." Yes, yes, yes. And we're comfortable with the wording. So, we want to delete it – sorry I've lost my train of thought. Are we striking it?

Kathy Kleiman: Can you just put a strike line through?

Emily Taylor: Okay, and just a reminder, we felt that we captured that will all. So next bullet point – "ICANN must establish clear and consistent rules", and we made a note for ourselves about timeframe which we can revisit, "for accreditation for privacy service providers that must include…"

Kathy Kleiman: Can I suggest an alternate concept since we've – this is really about introducing the bullet points below, and I've already lost it. So a minimum…

Emily Taylor: Ooh, I know what to do. Can I suggest that we put a colon, if we go up to that paragraph – or sorry, put "to include the following" sorry. So, "ICANN should develop and manage a system of enforceable requirements for all privacy providers (comma), to include the following", and then delete up to the first sort of sub point. Would that be…Bill?

Bill Smith: I'd like us to have "clear and consistent" in there somewhere.

Emily Taylor: "Clear, consistent and enforceable requirements".

Kathy Kleiman: Wait, we've got it below. "ICANN must establish…"

Emily Taylor: It's just about to disappear, Kathy. No, no, no. We are keeping all this up a little but not the intro; we're making that the intro. Are you comfortable with that?

Kathy Kleiman: Oh sorry, yep.

Emily Taylor: Yep, okay. So that means that if we take that then can you strike through, or actually are we comfortable just deleting the wording "ICANN must establish clear and consistent rules for accreditation that must include", because I think we've just captured all of that yeah. Just delete; just lose. Kathy.

Kathy Kleiman: Flag – old techie – "flag" means setting a bit off. So let's change the word "flag" that was a shorthand to "must clearly identify" or "clearly label that this is a privacy registration" – "private registration" or a "privacy", whatever. "privacy service registration"

Emily Taylor: Okay, so that is, we're now running through what the mandatory requirements, the clear, consistent and enforceable requirements will be – will include "WHOIS entry must clearly label that this is a private registration". Let's go concept and then wording. So

let's take a run through on the concept here. Okay. No, you've done nothing wrong. So, happy? Yay! "Privacy service must provide full contact details for itself, including name, address…" Lutz.

Lutz Donnerhacke: Why do we need this?

Peter Nettlefold: Well, full contact – so what are we saying? "Full contact details for itself"; so I guess one way of phrasing the question, are you asking because they will have already put the contact details in the registered name holder boxes because that's where their contact details will already be presumably. Is that the question?

Lutz Donnerhacke: You are asking for details to reveal the real identity here, not the contact details of the company running the privacy service itself? That's a completely different issue.

Peter Nettlefold: It is of the company, it's not – so you're registering with a privacy service that will hide, limit, whatever word you want to use, some of your details and out theirs in. But the details of the company should be available. So if you're a company providing a service then you're identified. It's a business registration step I guess.

Emily Taylor: Lutz, have I understood you, your concern is that this bullet point means that the registered name holder must provide full contact details?

Lutz Donnerhacke: No. My problem is I do not see a need in putting the information on the privacy service company in all those fields; we do not need those in this forum. We only need the contact, the relay contact in order to get information. We do not need the information who is running the privacy service itself.

Peter Nettlefold: How are we going to get a privacy service to follow mandatory guidelines, blah, blah, behavior if we can never find them if they don't?

Lutz Donnerhacke: Quite asking different. Do you fear that two privacy services hide their contract deals by each other?

Kathy Kleiman: Yes.

Lutz Donnerhacke: So we need the spanning tree?

Kathy Kleiman: I think we're saying "the buck stops here". If you're putting your data in…there is one problem here. Let's think of a way to generalize this a step, because we haven't told the ICANN community exactly which registrant fields have to be published. We've said as a minimum "registrant name", but they may decide "registrant name" and "phone number", in which case the privacy service would not be entering the phone number; so, just pointing that out. Anyway, I don't know what the wording is and it gets us down in the details, but I think we are asking the privacy service provider…

Lutz Donnerhacke: I'd like to make clear what my problem is. I can think of a privacy service which is running by a small company which is not available, but they have a service which is available in this time in order to reveal the private information if necessary. For instance, they hire a call center. That's a completely different issue and I want to only make to understand for me why it's important to have the information of the organization behind instead of the information we are requesting.

Emily Taylor: Kathy and then Bill please.

Kathy Kleiman: Lutz, my doctor is available 24 hours a day in an emergency, but in the middle of the night it goes through the call center because I

don't have her direct phone number. But that's not, that's still my doctor being available 24 hours. So if there's a relay service I'm not sure it's just an additional step. But if that relationship is contracted to the privacy service provider who can get the call, if there's something really going wrong on a domain name in the middle of the night, or if Bill needs to get to somebody, or Susan, if there's active fraud – as long as that message is relayed and wakes up somebody in the middle of the night then I think we're okay.

Emily Taylor: Can I try to cut through this? Because we are, we're under time pressure. Lutz, are you objecting to the concept of the privacy service being contactable?

Lutz Donnerhacke: No, but I don't see that it's necessary for who will contact the privacy service and get work and we should concentrate on the minimum system which is necessary to make it work.

Emily Taylor: I've got Bill and Wilfried.

Bill Smith: These services, once we introduce this type of service it is used for all types of things; for trademark issues, for security issues, for malware – yes it is. There is no other way to contact the

individuals that sit behind it. And by the 24/7, and I doubt that that will live that way, what I am trying to put in, or out is something that says there is an expectation of service level agreements on these things. It is not acceptable to sit for days on things that come in, whatever they are, you need to be available. This is an important service that you are providing for the domain name system, a fundamental piece of the internet.

Okay? You're a small business, fine. Hire a service to answer your phone for you in the middle of the night.

Emily Taylor: Okay, let's have clear, crisp interventions from everybody because we need to just focus on the issues where we disagree. Wilfried and then Lutz and Susan.

Wilfried Woeber: A question regarding consistency. I don't have a particular point of view regarding 24 by 7, 365. My question is for consistency again. Are there similar requirements in place for the rest of the machinery, for the regular registrations, for the registries, for the registrars? I presume for the registries the answer would be yes. For the registrars, I presume the answer would be no. So, the question actually boils down to, if my feelings are correct, do we want to install, for this particular special case do we want to install something which is more stringent than for the rest of the thing? And if we say yes, we should do it consciously.

Emily Taylor: That's a very good point. Thank you Wilfried. I've got Lutz, Susan, Peter and Bill.

Lutz Donnerhacke: We already could move technical details from privacy services in order to make short and direct contact in the case of an emergency, in the case of a security breech or technical issue. So taking Bill's argument into account, we have the response to trademark issues, or something like this. And I do not see a need to contact a company behind the service for such issues if the service itself has no obligations to be available at this time.

Emily Taylor: Susan, Peter and Bill. And I'd like people to think about a way through this please.

Susan Kawaguchi: This is Susan. So, if' I'm understanding you, you want to put the minimum amount of information in this registration?

Lutz Donnerhacke: A minimum set of obligations which is needed to put on the system in a consistent way.

Susan Kawaguchi: Right. So, a domain registration requires certain elements, so it has to be the privacy service contact information or it's going to be the person asking for the privacy service. It's got to be one or the other. There's no other option.

Lutz Donnerhacke: That's exactly the point here. I have no problem with an obligation that a privacy service has to provide contact for revealing the registrant data. I have a problem with availability for the company itself. It's completely different issue; running a service and being a company is completely different. It's similar like you are running Facebook. It's doesn't mean that all your service you are running, doesn't mean you are available all the time on the phone.

Emily Taylor: So it's not the concept of putting in the name and address and contact details, it's actually the 24 x 7 contact that you're querying?

Lutz Donnerhacke: What I expect here is there must be the contact details in order to reveal the information. It's not the service. The company running the service, we need an obligation that the service is available, not the company. That's different.

Emily Taylor: Okay, on my list I've got Peter and Bill please.

Peter Nettlefold: Yeah look I was almost going to pass it on, I was going to say, I just wanted to check, the only issue we're arguing about is the 24/7 contact or all the contact details?

Lutz Donnerhacke: Doesn't work in this way.

Emily Taylor: From a personal point of view I need a comfort break. So can I just ask you to try – because I still don't understand the point you're making Lutz, so could you try to explain to the others in a short break and then let's reconvene in five minutes?

[break]

Emily Taylor: Just a reminder, I think we've had a few people on the remote asking when we're going to finish up today; we have to finish up at quarter to seven. So we will go through until we've finished all our recommendations or quarter to seven, whichever is the earlier. Okay, Lutz, you were going to propose some alternative wording for this one that we've got stuck on. Thank you. I think that's good. Peter?

Peter Nettlefold: My only question and I thought this is what you were getting at so I agree this is something we missed, so thanks for picking this up. My question is phone and email, should it not be the full detail?

Lutz Donnerhacke: Only to suggestions.

Peter Nettlefold: Yeah, basically to fill in all the gaps, yeah.

Emily Taylor: Perhaps we could say "provide the contact details including"…

Peter Nettlefold: Yeah, thanks for picking that up. That's actually a good point that we missed I think.

Susan Kawaguchi: And I mean they do need to, and like he said it's only two details that he's brought in, so maybe he was figuring on this, but they do need to accept mail service. And a lot of privacy and proxy service will not, they proactively say "We will not accept mail service" and that's a problem.

Emily Taylor: Would it be solved, can I suggest by "privacy services must provide full contact details for itself"… Well we're talking about contact details which are required by the WHOIS, so let's focus on that. Wilfried and Peter.

Susan Kawaguchi: So maybe just address then. I'd be fine with that.

Emily Taylor: "Contact details as required" or "Full contact details as required by the WHOIS records".

[background conversation]

Kathy Kleiman: … the privacy services, we don't know, this fills in the gap. Yeah.

Wilfried Woeber: Now I'm completely mixed up. What's this information for? Which entity do we want to receive this information for? For the service provider? For the protected domain registrant or…I'm lost.

Peter Nettlefold: Because I made a real effort to try and understand this and so I'll say it on the assumption I may be wrong and if I'm wrong that's great, because then I'll need to try and re-understand again. I think

what Lutz has said is, and I think this is a completely separate question to the other issue we were debating about the step above, which is "the privacy service must provide its company details" etc. I think what Lutz has identified is potentially a gap where we said "privacy service by effect limits some of the registrants contact details", but what we never said, what goes into the vacant fields when the registrants contact details weren't there.

And I think what Lutz is saying is what needs to be there are the missing contact details and they need to be responsive. Now, there's a separate question about whether the company that does this service provides its physical address and ladi-da-di-da. But for the WHOIS record, what we saying is, don't forget to fill in the gaps and those gaps must be responsive. And in being responsive they may do various things.

Then there's a separate question, I think to me, that we know who these companies providing these services are. And the two questions are linked, but I think we missed this one.

Wilfried Woeber: So what you are saying actually is that this can point to a third party; neither to the domain registrant nor to the service provision company.

Peter Nettlefold: Well, that's why I say linked. I haven't thought through exactly how it works. But if there's a privacy service that offers the

service and puts details in here, I'm still interested that we know who the privacy service is; whether that has to be in the WHOIS record or through another mechanism. I guess I'm vaguely agnostic so long as if the privacy record says something and we can contact them and then we say "okay, who are you" – look I don't know how it works, but I guess the easiest way is, well I don't know because the easy way for the registered name holder is not going to be the name of the company, it's going to be the registrants name. So we do need a link between the two, but we can let someone else figure that out can't we. I don't know. Am I right?

Emily Taylor: I've completely lost my train of where that we are and I fear that we've got angels dancing on pinheads here and it's that we're going to be here for the rest of our lives talking about this.

Lutz Donnerhacke: What happens – you are looking up a domain name and getting WHOIS record. In WHOIS record we find a flag…

Emily Taylor: This is – Lutz, please.

Lutz Donnerhacke: We are writing down what we are expecting to see on the WHOIS record at the moment if privacy services are involved.

Emily Taylor: Lutz we are getting very bogged down in very fine detail here. Our scope is to review the extent to which the policy and its implementation is effective and meets the needs of law enforcement and promotes consumer trust. If we're going to go down to this level of detail on everything we are going to be here forever. Now please, can we just focus on getting through to the rest of these recommendations? If we have to highlight this text to something we revisit, fine. I do not think, honestly I've tried very hard over the last hour to understand this point. I do not see it as a show stopper and what is going to happen is this is going to stop this show and prevent us from reaching agreement. And I think that that would be a real shame.

Lutz Donnerhacke: So then remove both points because they are going in too deep and just delete.

Emily Taylor: Bill.

Bill Smith: I'm happy to have any of the language changed. I have no sense of ownership on the language. The objective for this, for me, is that in directing or suggesting that ICANN clean up the mess that they have allowed to grow in this space, they need to make it better.

People need to be accountable and we have to have enforceable—if not by contract, but by some other mechanism—ways to ensure that we don't get a recreation of the mess, or as best we can do. I am concerned that some of the changes I'm seeing are cutting all of the teeth out of this.

Kathy Kleiman: Can I make a recommendation? Can we come back to this? Let's italicize it, not even yellow it. Let's go through everything else and it may give us some sense of -

Emily Taylor: Okay, if we italicize those two paragraphs then we can revisit. There's some extra text that needs to come in. If you re-paste Lutz's suggested text and it's full, then we've got… That's what Lutz originally suggested. I think we lost a bit.

Okay, we'll go on to the next one. We'll come back to this area. Standardized relay and reveal processes and timeframes. And we'll obviously construct a sentence around that. Rules for the appropriate level. In fact, we don't need one, do we? Sorry. Rules for the appropriate level of publicly available information on the registrant.

Now, this might actually be the point that we're talking about, which I think might solve your concern, Lutz, is maintenance of a dedicated abuse point of contact for the privacy service provided,

because that doesn't actually have to be, then, does it? It can be third party.

Kathy Kleiman: It can be their attorney, not inside council. Does that address your concern? The maintenance of a dedicated abuse point of contact for the privacy service? But you don't object? Okay. Good.

Emily Taylor: Privacy service provider shall conduct periodic due diligence checks on registrant contact information. There must be a balance between privacy and security. Heighted bar, SLAs, 24/7. So, right. Is this a wording issue or is it a sense you don't believe there should be a balance between privacy and security?

Lutz Donnerhacke: You put security out so it has no meaning here.

Kathy Kleiman: The point, really, is that the group that's considering the rules has to take into account the needs of law enforcement in the security industry. Those last words.

Peter Nettlefold: Just provide explanation and obviously they're not the right words. So, this is the bit when I was trying to explain it all before, where

this is obviously a broad policy framework and there's going to be a bunch of stuff that's missing.

One of the things that is missing that is very clear, which we're not going to solve, is the threshold for revealing the underlying data. In that particular case, in coming to that decision, they need to balance the privacy and the needs of law enforcement and others, so there is a need for the data in some cases and there is a need for privacy. In coming to deciding the balance on when it is reviewed or protected, they need to consider both. It's poorly worded, I agree, but that's this incident.

Wilfried Woeber: I'm wondering, shouldn't this rather go into the bullet point or into the section on the reveal process?

Emily Taylor: Bill.

Bill Smith: Absolutely. The wording on this is very poor. It was captured very quickly. In fact, I threw it in while I was sitting here at the start of the meeting to say I remembered we forgot to add that. But basically, it's a comment to the community that, forget the words I'm using for this, but -

Emily Taylor: I think Peter might have some alternative text to suggest.

Bill Smith: Okay.

Peter Nettlefold: And an alternative spot as well, because now that we see it, it's at the end of all the detail stuff. So, I'm suggesting, if we go back up to the start of this dot point list, Alice.

So, ICANN should develop and manage a system of clear, consistent enforceable requirements for all privacy service providers. Full stop. After providers, full stop. This should balance the needs of privacy, law enforcement. Do we want to focus on those needs? This is a question, me speaking out loud, or do we say there needs to protect or reveal data in certain situations? So, we want the needs of the stakeholders or do we want the needs of -

Lutz Donnerhacke: Simply leave it out. Balance.

Emily Taylor: We have to balance something. I think you need to -

Lutz Donnerhacke: My question is… My problem with the last point on the list is if they have security here, if we put out all technical issues before,

security can only mean terrorists. I do not want to have such a discussion here.

Peter Nettlefold: No, we're not having that discussion, Lutz, so I think it's clear we're not talking about that so we've got to move on from there. The question is if I'm a person and come up and say I want the data, do I get the data?

Does me just asking for it outweigh the privacy concern? Probably not. If I'm a law enforcement official and say, "Here's a court order. This person has killed someone, is peddling child pornography material," do I not get the data? Clearly not.

So, there's got to balance the needs to either protect the data or release the data. We need to, as we're providing high-level principles for this policy, we're just saying as you are considering developing this policy, you need to balance these two things. That's all it's saying.

Lutz Donnerhacke: It's far out of our scope.

Emily Taylor: We were on a telephone conversation with one of the signatories of the AoC in January and one of the clear messages I took away from that conversation was that the reason for putting it into the

AoC was for us to assess whether the WHOIS service currently achieves the correct balance between private citizens' rights and expectations of privacy and the needs of law enforcement and others who might want to make a contact with that person. Seth.

Seth Reiss: Bill, Kathy and Peter did something that furthered the whole group and they worked well together and came out with compromises that enabled us to move very quickly forward and I think we should try to achieve that again.

So, we should try to make proactive comments to the extent that we have concerns. We should try to figure out a way to get through those concerns, either by working on wording later on for our final document, rather than have those concerns be an obstacle to achieving what we hope to achieve in the next half an hour.

In other words, put some of the terminology concerns, or even philosophical concerns, aside to the extent that maybe the future discussions can resolve them for the final document so that the rest of us can achieve what we hope to.

Emily Taylor: Thank you, Seth. I think we're looking for something to capture the concept of balancing these. Peter, you suggested something which I've now forgotten. Privacy and law enforcement, but you had an alternative, which was balance the requirements to protect

individual privacy versus revealing inappropriate circumstances or something.

Peter Nettlefold: Yeah, I think so because in saying that, I didn't want to start again on the parts of privacy law enforcement, then I thought it's not just law enforcement. And then I was thinking what our scope was, which is legitimate needs of law enforcement to provide consumer trust.

That's not really going to work in this situation, so I thought instead about what the actual actions are. So, it's to balance the need to either protect or reveal the information in certain situations.

Emily Taylor: Or in appropriate circumstances.

Peter Nettlefold: In appropriate circumstances, something like that. And again, we're not developing the policy here. All we're really saying is in developing the policy, there's clearly got to be a balance when you hide the data or you don't hide the data. Okay, excellent.

Emily Taylor: I've got -

Wilfried Woeber: Yeah, very much in the same direction that Peter has proposed. My suggestion for wording would have been to balance the need for privacy against valid requests for disclosure of this information. Valid requests for disclosure.

Kathy Kleiman: The agreement with law enforcement community and the industry around law enforcement.

Emily Taylor: So, that's a specific -

Kathy Kleiman: The agreement this morning, at least outside, was about was about law enforcement and the private industry around law enforcement. Valid request is, oh, my God, it's in the eye of the beholder, I'm afraid.

Susan Kawaguchi: Because I think we're not too far off. So, if an IP owner can see the registrant name, so we're halfway there. We have something to hang our investigation on. I might get brutalized in the CSG here, but…

So, I understand why you would like to limit this to law enforcement because there's enough issues with just limiting it

with law enforcement asking for this. I'm assuming that this will be a very narrow subset of Internet users that would want to use this privacy service.

My only concern, and I can't give you language right this second to address this, is there is often many times eBay, PayPal, Facebook are part of that legal law enforcement investigation, but because law enforcement doesn't have the resources, we have to do that research.

Kathy Kleiman: We say that privacy policy law enforcement and the private industry around law enforcement. Then the community will push to expand it. We know this.

Susan Kawaguchi: But I think there's definitely a need for all of that and I think you did capture that.

Kathy Kleiman: Balance the needs of privacy, law enforcement -

Emily Taylor: And the private industry around law enforcement.

Peter Nettlefold: I just have a question. Why are we limiting it to certain cases? I don't want to be difficult, but if there's a reason to reveal that is valid and part of the scope is consumer trust and we're talking about people being able to… Why are we all of a sudden saying the only people that can have the data are law enforcement?

I'm here to say that it's very important that they do, but I'm not sure that we've seen anything from the community or that any of our studies or anything that we've got fact-based that says we should be limiting it just there. Bill's got his hand up.

Bill Smith: I'm happy if the information disclosure is the way it is. The thing for me, the balancing act is actually at a higher level and I've tried to scribble down some thoughts on this. Again, don't take some of the words explicitly.

The concept is we need to balance the individual's right to privacy with the community's right to social order. That's the tradeoff. In a community, yes, you have a right to privacy, but you enter into a social contract as part of the community that says I will give up some rights, a certain limited set of rights, for the benefit of the community because I get some things. I get security; I get a known way of things happening. I get order.

That's the message I'm trying to get that needs to be taken into consideration. It's not just cyber security or IP this, it's how fast

are you going to respond? If you're going to take 15 days to respond, that may not be good enough. If you're going to respond in 15 minutes, I might accept something else. Those are the things that people need to consider.

Peter Nettlefold: If we're happy to have the balance thing in, and if people are happy with the principle of balancing and we know that we're talking about actively hiding the data or revealing the data, maybe we can… Again, if we agree on the principle, we can do the words and anything elsewhere.

I heard Bill's thing. It sounded okay. I'm not really sure what social order means or whatever, but something along those… I think we can wordsmith that elsewhere. If we agree there's a balance, it's a high-level principle that we need to somehow reflect, can we just bracket it and do all that stuff and sort it out?

Bill Smith: So, a definition, right? Social order. Relatively persistent system of institutions. Patterns of interactions. Customs capable of continuously reproducing at least those conditions essential for its own existence.

Kathy Kleiman: We're in political and social theory now.

Bill Smith: If you're talking privacy, that's where we are.

Susan Kawaguchi: So, Peter, you had said, "Why are we limiting it?" earlier, I think. I can't really say, I can just say how it is now. So, for a proxy registration, like a domains by proxy, you have several choices here—I want to report a domain that infringes a trademark, sending spam, content infringing on a trademark or copyright, defamatory, libelous or other objectionable content.

So, there's certain categories. Just because I don't like what they have on a site, I have no right, unless they're infringing my trademark, to ask for the proxy registration information to be revealed.

Peter Nettlefold: I get it and I don't think that we should just accept… This is part of the current system which is busted, or maybe not busted, but I see no reason that we would accept that definition as part of the new system that we're proposing be developed.

So, if a new system is going to be developed to tidy this up and it's going to involve making sure we know who people are and they're going to defy standard processes, then part of that would be finding this balance appropriately.

Were all the correct privacy people in the room when that was developed? Were all the law enforcement people in the room when that was developed? I doubt it. If we're going to fix this, then we need to make sure that they are and they fight it out together and come to the right balance.

Seth Reiss: So, to achieve the high level balancing generality, because it's very difficult to come out with a detailed scene that's going to satisfy everybody and I don't think that's our… I'm sorry? Go for it.

Emily Taylor: Manage a system of clear, consistent, and enforceable requirements for all service providers, comma… I'm sorry, keep privacy there. Comma, which strike the appropriate balance between the different stakeholders competing, but legitimate interests.

Kathy Kleiman: I think we did a really good job this morning of -

Emily Taylor: I think you did a great job.

Kathy Kleiman: - law enforcement. We're going to hear from a lot of other community… Just so you know, I would get calls constantly and

emails constantly, “This information on the website is not accurate,” or, “My ex posted this and take this down.” I don’t know what a valid… I really want to make sure law enforcement’s in the room. We really want to make sure private industry around law enforcement’s in the room.

I think in a lot of ways, that would include intellectual property attorneys. I’m not sure. They should get back to us and tell us whether they think that includes them. It would certainly include the fraud folks. That’s where we’re starting.

Emily Taylor: I think, Kathy, that’s what I’m trying to aim at by trying to do what Bill was also trying to do, which is take it a step higher and not actually define who the different stakeholders are or what their different competing legitimate interest might be, but to recognize that there are competing but legitimate interests and as these rules and systems are developed, that they should identify and balance those competing but legitimate interests in the regime that emerges. So it’s not trying to second-guess or predefine what that is.

Kathy Kleiman: Legitimate interest for me to have incorrect information posted by an ex out there.

Emily Taylor: No, it's not. No, it's not.

Kathy Kleiman: According to some people it's…

Emily Taylor: But, Kathy, this is about legitimate. It's limited by saying these are legitimate interests. It's not trying to define what those interests are.

Seth Reiss: And be able to define that in this table.

Kathy Kleiman: Can we take the whole balance thing out? Because I was the one trying to put it in based on wording we had had this morning and agreements.

Emily Taylor: I think no. I think it's important to have it.

Kathy Kleiman: But basically saying balance everybody. We were giving some direction for the minimum framework of the groups most important to be contacted.

Emily Taylor: Okay, well, how about this, Kathy, that we somehow try to unravel and find all the original wording and just put at a minimum, the blah, blah, blah, blah, blah, blah, law enforcement and privacy. At a minimum.

Seth Reiss: So, the next sentence would be at a minimum, this would -

Emily Taylor: At a minimum, this would include individuals, privacy and the needs of…

Peter Nettlefold: I just want to know the -

Emily Taylor: Peter, please don't.

Peter Nettlefold: I just want to -

Emily Taylor: We can't get into hours of debate about NGOs and -

Peter Nettlefold: But, I don't -

Emily Taylor: It's about -

Seth Reiss: It's about compromise. We have to give each other a little bit of room.

Emily Taylor: We can certainly take out individuals. I don't…Kathy, how about at a minimum this would include privacy, comma, law enforcement and the private industry around law enforcement, and then we finish it there?

Kathy Kleiman: Can everybody live with that?

Emily Taylor: Can we live with that?

Seth Reiss: I think it's important to realize we can continue to argue about this after today.

Emily Taylor: We will always continue to argue about it.

Kathy Kleiman: I think we should just publish after today.

Emily Taylor: Welcome back, Sarmad. I think this now reads, "ICANN should develop and manage a system of clear, consistent and enforceable requirements for all privacy service providers which strike the appropriate balance between the different stakeholders competing"…if you remove "with". Yeah, "Competing, but legitimate interests. At a minimum, this would include privacy, law enforcement and the private industry around law enforcement," and then finish.

Kathy Kleiman: I think this is really going to help the community.

Emily Taylor: Fine.

Kathy Kleiman: Great, because it's the only that's been around for a long, long time.

Emily Taylor: That's good. And then, Alice, if you could, just before the blue stuff, starts, just put a full stop and then delete the rest of that.

Kathy Kleiman: Thanks for everybody's patience.

Emily Taylor: We should probably just… no? Is that a thumbs up or down? Down.

Lutz Donnerhacke: Private industry around law enforcement's not under our scope. I already tried to say this. I do not have a problem with consumer trust here.

Emily Taylor: Okay, what about "at a minimum, this would include privacy, law enforcement and consumer trust"?

Kathy Kleiman: Can you view above? I think that very wording, "private industry around law enforcement" is in our findings. Isn't that right? So, we're pulling it down from the findings into… Private industry around law enforcement. Let's see.

Emily Taylor: It's already a low and it's just highlighted. I think most of us here are comfortable with that and you are querying on the private industry around law enforcement. So, if we just note that.

Lutz Donnerhacke: That's the ongoing discussion point if it's included or not, then I do not want to have it here.

Emily Taylor: Please, Alice, don't cross it out.

Lutz Donnerhacke: Make it purple.

Emily Taylor: Just make it purple.

Kathy Kleiman: Yeah, and please keep that.

Emily Taylor: Bill, please come to the mic.

Kathy Kleiman: Could you un-strike it?

Bill Smith: I understand that Lutz doesn't want it in there. Can he please offer a suggestion for those who actually act in support of mitigating or eliminating fraud, malware distribution, botnets, denial of service attacks, et cetera?

Lutz Donnerhacke: We have a common misunderstanding between our…understanding how law systems are working here, and I do not want to have the discussion on the table. It would take too much time. We in Europe have to understand if it can't do it in a private way, we go to the authorities. Other countries had other implications how to deal with this and every council offered on the table here.

Emily Taylor: Kathy, did you want the mic?

Kathy Kleiman: Yeah, I'm typing it to Alice, but Alice, I think we're un-striking. We're keeping it in purple, but we're un-striking it because it's very valuable information.

Emily Taylor: Thank you. Let's power on. We've highlighted that it's problematic and let's continue. If you keep going down. I think we've gone beyond that. We've gone to the twenty… so, that was thumbs up. We reached the "after consultation with the community, ICANN may require publication."

Peter Nettlefold: Above that.

Emily Taylor: Yeah.

Peter Nettlefold: Adopt the SLAs and stuff can be deleted. I think that's what we debated up higher. So, Alice, that one that you've highlighted, it's my understanding, anyway, that that's what we were trying to wordsmith up higher, so we just can delete that. Strike it, yeah.

Emily Taylor: Okay, Sarmad?

Sarmad Hussain: Are we on the yellow highlighted portion?

Emily Taylor: Yes, I think we are now at the yellow highlighted portion.

Sarmad Hussain: So, even though I drafted this, I do want to add that if appropriate mechanisms are put in place, this may become redundant. What I'm saying is if appropriate measures are put in place for privacy services where they're required to do certain things, under regulation, then this becomes redundant.

Emily Taylor: Are you proposing to strike it?

Sarmad Hussain: Yes, there's a possibility, but this was originally also Lutz's idea, so also get his feedback.

Emily Taylor: The wording may require…it doesn't suggest that this is definitive or that it's compulsory, so it's just more of an observation, I think. So, it might not be necessary to your point. Kathy.

Kathy Kleiman: Is there a way of flagging this particular field as saying for security and stability reasons? We'd like special consideration of the technical contact. Or doesn't it matter, guys? Bill? Lutz? Anybody? But, I thought this was the point Dr. Sarmad was trying to make, so I was trying to capture -

Emily Taylor: I think Sarmad was trying to capture a different point. Let's just take it out.

Kathy Kleiman: Drumroll for the final point.

Emily Taylor: Final bullet point. We haven't slugged it out on the definitions yet, so let's not be too previous. "ICANN should develop a graduated,"

and, by the way, before I start this, this is text that we're familiar with from Marina Del Rey.

Kathy Kleiman: Number 42.

Emily Taylor: "The concept of graduated and enforceable series of penalties for privacy service providers who violate the terms of their accreditation with a clear path to de-accreditation for repeat, serial, or otherwise, service breaches." So thumbs down from Lutz. Query from you.

Sarmad Hussain: So, I think what we need to do is first graduated steps to audit it and then a penalty before having graduated steps of auditing. It's sort of hard to have graduated steps for penalty.

Emily Taylor: Lutz.

Lutz Donnerhacke: It's already included in the word enforceable.

Emily Taylor: Actually, I think that the concept here is the graduated steps, which is something that we've discussed in the context of the tools available to compliance, so it's not the –

Lutz Donnerhacke: So then starting from the word "terms," "violate the requirements," period.

Emily Taylor: Bill.

Bill Smith: So, by removing accreditation earlier or anything that's contractual, we have rendered virtually all of this stuff unenforceable. There's nothing ICANN is going to be able to do at this point. It's just the way the system is today.

Kathy Kleiman: So, we've set up mandatory requirements about…right? Mandatory enforceable, so I think all we're doing is changing the word "accreditation" to the "mandatory enforceable requirements," it seems to me. Accreditation means x, but there are lots of ways to certify; there are lots of ways to accredit. You can do it with contracts. There are lots of ways.

What we're doing is saying however you've agreed to apply by the requirements, we're yanking that and now registrars can't

participate with you. There's going to be requirements, there's going to be somebody holding themselves up to have those requirements, to follow them, and there's going to be a loss of that right.

Peter Nettlefold: Again, I want to understand why Lutz's thumb is down. Is it because you think it's already covered? Or is it because you disagree? If it's already covered, it's a belts and braces thing. Do we need to really argue about it, or do you actually disagree with this?

Lutz Donnerhacke: I want to remove that part that's accreditation. Starting from the word terms up to the final of the bullet point using the requirements. Full stop. We have to use the term requirements and above so we can use it again.

Emily Taylor: So it would be "violate the requirements," full stop. Delete the end because the argument is that we have included the concept of de-terminating, whatever we want to call it, deactivating these people. Bill.

Bill Smith: Requirements, I don't think, would catch repeat, serial, or other service breaches.

Emily Taylor: Can we just have a look and check? Can we highlight the… "The repeat, serial, and otherwise service breaches" was quite a strong message. This is text we've lived with for quite a long time.

Personally speaking, I like it. If we change "terms" to "requirements," and "terms of accreditation" goes, Lutz, can you live with "with a clear path to de-accreditation" or "termination" or something for repeat, serial, or otherwise service breaches?

Lutz Donnerhacke: I have no problems and especially mentioning to Peter breaches or something like this.

Emily Taylor: Okay, so we can just… Alice, could you un-highlight and un-score out from "with a clear path" to… Okay, that's now accepted. That's our recommendations on proxy and privacy, guys.

Peter Nettlefold: We missed one.

Emily Taylor: What? The definitions below or we've missed one out?

Peter Nettlefold: We had talked and I was going to draft the wording for an affirmative statement, but do we still want that in? The affirmative statement.

Emily Taylor: We did.

Peter Nettlefold: Yeah, and I actually have some -

Lutz Donnerhacke: The accreditation's still in. With a clear path… maybe it's…go down, please.

Bill Smith: Are we going to go back on the definition of law enforcement and those in private industry who work around it at some point?

Kathy Kleiman: Can I explain why I wanted the more narrow wording? We've been debating for ten years the validity of lots and lots of different requests to…against for WHOIS data, for privacy. It's hard. It differs by country and it differs by who's asking and receiving.

One of the things that I've noticed across the community, and I say this with my old registry hat on, is that when the request comes from law enforcement and those working in the cyber security

industry, be it government or whether it's CERTs, private or public, whether it's fraud, this rises to a different level.

I'm not saying intellectual property isn't important. I've gotten a number of legitimate—and illegitimate requests, frankly, from my point of view—but these particular issues rise to the fore, and if we tell the community to focus on this, we will help them break a lot of damage done in the last ten years.

If we tell them to focus on anything, we're going to be mired in the same place. If we tell them to focus on this you can even say, if we want to call it industry and government around cyber security—because that covers CERTs—but whatever you do, if you're covering Susan and you're covering Bill—I know that lots of IP guys are listening; I'm not excluding you—but I'm saying the minimum, tell the community to move forward on this and we're going to have something.

Thanks for Peter for helping me understand why I was so concerned about this.

Peter Nettlefold: And I thank Kathy for helping me understand, and now I can see why she was trying to narrow… I think, yeah, potentially, there's a threshold question about the way the wording is. I certainly know from my stakeholders they're very keen to be included, which is

initially why I was keen not to narrow too far. And I also understand people like Bill and Susan and so on.

So I guess it's a question of partly wordsmithing, partly deciding where in helping the community we make that threshold. I don't have the solution, but I wanted to thank Kathy for helping me understand what we were talking about.

Emily Taylor: Who has got a problem with the wording "private industry around law enforcement" on the basis it's not ideal wording? But "the industry around law enforcement," and then you don't have to inquire whether it's…

Lutz Donnerhacke: Could we have something like "law enforcement and supporting organizations," or something like that?

Peter Nettlefold: How about "the cyber security industry"?

Lutz Donnerhacke: That's the kind of worms I do not like to augment. That's the kind of worms I do not like to augment. There are a lot of people there claiming to be doing something lawful or helping something lawful. We have a different understanding what's allowed and what's not allowed and I do not want to have a motivation for

some people who think they are allowed to do the law by themselves in the document here.

Peter Nettlefold: I'm interested and I understand where you're coming from, but as a technical person, you would have an interest if the DNS was being abused, I expect, and that had a cyber-security implication. For example, would you contest a national CERT accessing WHOIS data for a legitimate reason?

Lutz Donnerhacke: Not really. I have no problem with a national CERT. I have a problem with anti-spammers.

Wilfried Woeber: I am mostly with Lutz here because the term "security industry" is much too wide. It's much too broad because this can easily be extended into intrusion detection systems and into statistics gathering and that sort of thing. I like this rather closed link to law enforcement in the wider sense because it provides a basis for the legitimacy of the request.

If you go into the broader security industry, you can have F-Secure, or whatever the company is, say, "We are in security industry. Please give us the data," and that's definitely not what we want.

Peter Nettlefold: I can say, in terms of reaching compromise, that if we can include CERTs, I'm pretty close to being there. But, I don't know where that leads, Bill and Susan.

Kathy Kleiman: Are CERTs included in this language?

Peter Nettlefold: I don't think they are, to be honest. From my understanding of the way it operates in Australia, we now have a national CERT, which is part of government, but I do not believe it would probably be considered to be law enforcement. That may well be the case in other jurisdictions as well.

Lutz may know more, to be honest, but in the Australian case, I don't think they are law enforcement, but they are part of government.

Sarmad Hussain: So, just thinking out loud, I'm going to go on Lutz's side now. Even if we say whatever we want to say here, if private organization person goes to proxy service to request for some data, the local laws will actually prevent that unless there is a proper legal document through law enforcement served to the privacy organization. So, even if we say this, can we actually enforce this? That's my question.

Susan Kawaguchi: I was just going to say in getting back to my list I read off at the domains by proxy, all of those are based at least in US law, so those requests, reasons that the proxy registration could be revealed, so for that practice, that's where that came out of.

You wanted to extend it. I think if we extend it too far you're going to run into (a) people having information divulged that shouldn't, (b) putting the privacy provider in a position where he's going beyond the law of the land.

[background conversation]

Susan Kawaguchi: No, and I don't understand why you would want CERTs, because in the US, you would not issue a CERT based on a proxy registration.

Bill Smith: This is the computer emergency response to -

Susan Kawaguchi: Okay, so I'm out of my element, then. Sorry.

Emily Taylor: Can we just try to think about the concept that we're trying to capture here?

Bill Smith: From my perspective, the phrase "private industry around law enforcement" wasn't the best, but it got the message across. In fact, many of us don't even want the information. Many of the issues we deal with, we don't care about the information. We just want something done. That's where the balance has to occur and the service level agreements.

If we're trying to do something around a distributed denial of service attack or malware distribution or something else, we want the issue resolved. I don't so much care about the individual or the entity behind it. That's, actually, the thing that I want to ensure that is taken care of.

If that means we have to have information revealed, fine. If not, if there's a way for the registry to do something, that's okay, too. That's the balance I'm talking about.

Emily Taylor: Okay. Yes, so talking about balance, don't forget we have the words "at a minimum" so we're already providing for the fact that this can be extended.

Michael's observation… I don't know, Michael, perhaps you can clarify whether you mean the entire set of recommendations or just this paragraph, but point well taken. I'm afraid the text becomes excessively complicated.

I do understand that we want to find a compromise, but if it becomes unreadable because of too many words, it would be difficult to understand what, exactly, we want it to say. That's true, and I think nobody particularly reads heavily negotiated documents as great literature.

What we're trying to do here is, of course, make our meaning clear, but also capture the concerns and the views of people around the table, people within the review team who have different views.

At the moment, we have the concept of balancing the right…balancing…what do we say? "Striking the appropriate balance between stakeholders with competing but legitimate interests. At a minimum, this would include privacy, law enforcement," and what?

Peter Nettlefold: I'm seeking guidance from elsewhere. I'll just read it out and if no one likes it, I guess if we all think it's not even a worthy starting point, we can start again. It's the GAC principles. "gTLD WHOIS services should provide sufficient and accurate data about domain name registrations subject to national safeguards, for individuals'

privacy, in a manner that supports the stability, reliability, security and interoperability of the Internet from a technical and public trust perspective."

Emily Taylor: I like that. Bill. Are you generally unhappy, or -

Bill Smith: Yeah, I'm generally unhappy. I think we've made the text based from what we had started this morning unrecognizable and I think we've taken most of the teeth out of it.

Removing or changing the private industry around law enforcement, that's a real problem because the industry around law enforcement, actually, is doing most of law enforcement's work right now and that isn't going to change in the short term. That may never change.

Lutz Donnerhacke: But, it doesn't mean that industry has the same rights as the law enforcement itself.

Emily Taylor: We can argue the toss about this, Lutz. I think that we can recognize that many people around this table have made many concessions this afternoon on the issues that they feel dearly about. Bill and Kathy and Peter did, I think, an excellent job of

balancing… Three people coming from very, very different directions, really, and coming to us with a set of text that they were happy with.

Kathy Kleiman: Or equally unhappy with.

Emily Taylor: Or equally unhappy with, absolutely. This is a point which, frankly, personally, I don't feel strongly about, but I can see that if I was sitting where Bill or where Susan are sitting, I would feel that a lot of my interests are already quite compromised on and that this is not something that, to me, makes the whole thing dangerous.

The shorter phrases are better. Let them be more numerous, less lengthy. Michael, thank you for that comment, and we have made a note to ourselves that we are going to check this for English, if I can say.

But, we do also have to accept that there are going to be some sentences that are heavily negotiated, where they will be not that brilliantly readable. I don't care. There, I've said it. So, what are we going to do?

Kathy Kleiman: Have a drink?

Emily Taylor: I would propose that we keep "and the private industry around law enforcement." I think, from Kathy's point of view, that you can live with that. From your point of view, you can live with that.

Peter Nettlefold: Can we just say "industry"?

Emily Taylor: "The industry around law enforcement"? Does that cause a problem? I know you're not happy, but this is about compromise and this is about leaving here with an agreed set of recommendations rather than not. I think they call it the dirty side of the consensus. Is that what they call it in America?

Susan Kawaguchi: I need to admit I was wrong on my… Doesn't happen very often. Ask my husband. So, whatever RAA I searched, I didn't search it correctly. The language about the reveal language was in there in 2001, so I am wrong and I am pulling that back.

I still am not quite comfortable with the proxy, the way we're going to handle it, but I will be okay. But, I just wanted to make sure everybody knew I was wrong on that.

Emily Taylor: That's very helpful and thank you for pointing that out, Susan.

Kathy Kleiman: I know observers in the room aren't commenting, but there's a comment online from somebody who's listening, Mark McFadden, that shares and talks about wordsmithing and that we may be obscuring… He said, "Nobody reading this for the first time would understand"…sorry, Mark's typing and just a longer quote…

So, something to keep in mind as we fix it and we draft. "Nobody reading this for the first time would understand all the background and compromises that led to the text being the way it is."

Let me just share with observers that we are writing an entire report to go with this, so I just wanted to… I'm with Emily. Let's go with what we agree with and we'll clean it up and we'll explain it later.

Emily Taylor: I think it may well be fitting to describe what we mean by the industry around law enforcement at an earlier stage in the report to make it clear. Sorry, Peter, you were asking for…

Peter Nettlefold: I only want the mic if we're finished with this one, so I'll just check first, because I'm going to change the subject. Are we done?

Kathy Kleiman: Do we need to get to definitions quickly? Because I thought there was a new definition from Seth that we were plugging in here and I'd like to do that.

Peter Nettlefold: That's exactly where I wanted to go.

Kathy Kleiman: Well, then we're on the same page. That's good, very good.

Peter Nettlefold: It is.

Emily Taylor: I think that the really contentious bits are now highlighted in purple, however, on the list of findings and recommendations, I think we have agreement, subject to the purple bits, and subject to the general cleanup for sense.

Kathy Kleiman: Is it still purple, though, or can we take this out of purple "and the industry around law enforcement"? I thought we have agreement on this now.

Emily Taylor: Are you proposing to take it out of purple?

Kathy Kleiman: Yeah, I'd like to take it out of purple.

Emily Taylor: Is Lutz going to die in a ditch?

Lutz Donnerhacke: We are living in a democracy and if the majority of the people are doing something that the minority might have to have an option, to say do the protocol and then do the same thing as the majority.

Kathy Kleiman: But, does that mean you can accept this? Okay.

Emily Taylor: Okay, so then you yield to the consensus view. So, let's go to -

Bill Smith: Sorry, Lutz is talking about a democracy, not consensus. I just asked him that question. We do not have consensus on this.

Emily Taylor: To clarify for Bill, please, Lutz, are you saying that you maintain your disagreement? Or that you yield to the consensus view, not including you?

Lutz Donnerhacke: I do not want to give a private organization the same rights as law enforcement just for doing something they consider fraud or breaking the law. So, we cannot have consensus on this point, but we have to make progress, so I step away and put it to the protocol that I do not have the same meaning on this point. I do not agree on this point. That's all.

Seth Reiss: It's not that you mind private industry as being included, but you don't want this provision to be read so that private industry has equal rights or equal importance to law enforcement. Is that correct?

Lutz Donnerhacke: That would be the consequence in writing it in this form here.

Seth Reiss: So, is it possible just to add a bit at the end?

Emily Taylor: Do you have proposed text?

Seth Reiss: I sounds like "at a minimum, this would include privacy, law enforcement, and to a lesser degree, the industry around law enforcement."

Lutz Donnerhacke: Let me shorten this. We had a discussion on the law enforcement definition team a month ago and we agreed to disagree on this point, so keep it as it is.

Peter Nettlefold: This is reminding me of a point which I think we all agreed on earlier. I just wanted to ask Alice to do a search or to check whether it's in the final text, because I think it may address some of your concerns, and that is that we had, as a principle, that this new policy must be in accord with national law. So, we wouldn't be allowing a private crusader to breach a national privacy law.

I would be very uncomfortable about that as well, but I haven't seen it on the screen for some time, so I'm wondering if we actually put it in. So, could we check? Sorry, the section we've just been argu…discussing, I think meant to have in there is one of the founding principles that the new framework, whatever we're calling it, is consistent with national laws, relevant national laws, applicable laws, whatever we thought.

I think we all agreed that that would be in there. I think it will address some of Lutz's concerns. I think it's missing. We may have just forgotten to actually type it in.

Emily Taylor: Where is it?

Peter Nettlefold: Where we just were, I think. So, to bubble the little dot point up, further up, so "ICANN should develop and manage a system of clear, consistent, enforceable requirements for privacy service." How about we put it there? "Consistent with national laws." Then full stop. Then we go, "This should strike an appropriate balance," I think because there's many balance points. This, I think, Lutz and I would entirely agree, we certainly, I certainly, and I'm sure most…all governments are very fond of their laws, so we don't want people breaking them.

So, to the extent that there is someone with a Superman outfit on trying to do something which would breach a privacy law or some other thing, we wouldn't be happy either. I think that the legitimate people at the table won't be breaching those laws, but I think your main concern with the private industry is that there are some people who may be looking to breach laws or do things which are illegal.

Emily Taylor: Yes, the vigilante -

Peter Nettlefold: I think you've already agreed with the text, but I hope this strengthens your agreement rather than -

Lutz Donnerhacke: If a company like Facebook or PayPal is concerned with a fraud problem, currently they are going to make a very fast way to take it down to stop this fraud, but normally they don't have the right to do so. They do not have the right to reveal a lot of information for this. They had some [bad orders] and that's my problem.

I do know that they are making it for a good purpose. That's not enough to have a good purpose. Defining good and bad is a matter of side, not a matter of policy.

Peter Nettlefold: Does that mean you're okay with including "consistent with national laws" or not?

Lutz Donnerhacke: If you remember how our executive and law enforcement people in Germany are currently behaving, I'm definitely not satisfied with this sentence because they are breaching their local law itself.

No, I do not know what to say on the sentence. At least leave me out on this. I have problems with it. I do not be able to express it in a very short form and to make a better solution here, so please leave it out. Let it be as it is and take my concerns to the protocol.

Kathy Kleiman: Just leave it on the record.

Emily Taylor: Can we move on? We've got 35 more minutes before I absolutely need to go, so could we move on to the definitions? And then I do want to spend a bit of time discussing the accuracy recommendations, which I had thought we had agreed on in Marina Del Rey, but when we started going through them yesterday, it seemed like we had completely reopened everything on them and I just want our confirmation that what is agreed is agreed.

Kathy Kleiman: Emily, are we moving on to this document?

Emily Taylor: No, we're not. We're going to just come down to these definitions because we haven't really discussed these in detail.

So, thank you very much, Seth, for providing text for an alternative definition of proxy, which you say is a business relationship in which the registrant is acting on behalf of another. The data is that of the agent, and the agent alone obtains all rights and assumes all responsibility for the domain name and its manner of use.

Just looking at it, my only query is that the term "the registrant" there is somewhat ambiguous what is meant, but Sarmad, you have a comment.

Sarmad Hussain: Is it a business relationship or a legal relationship, or…?

Wilfried Woeber: Do we really mind what the relationship is? If the responsibility rests with the registrant, I really don't care whether it's just a shake of hands or a business contract.

Emily Taylor: And, do we mean another registrant or another entity?

Kathy Kleiman: I liked leaving it open because be careful what your kids do with their domain names. It could be a private person; it could be an -

Wilfried Woeber: The term "the data" is not specific enough. It might be WHOIS data or registrant data or something like this.

Emily Taylor: We say the domain registration data, or, in fact, I think we're proposing, maybe, WHOIS data, consistent at the domain registration data.

Wilfried Woeber: I think this should be one of the very last exercises to take care of these approbations and these things. As we said a while ago, we are probably going to adopt the recommendation by the SSR or minimum security, Security Stability Advisory Committee. In particular they are talking about domain name registration data.

Emily Taylor: Susan's been waiting a while, so let's go with Susan and then Kathy.

Susan Kawaguchi: Defining the data was important, so however we decided on that is fine. In the RAA, they do not use registrant, they use registered name holder, so if we want to be consistent or not, but I think everybody in the industry knows registrant is the registrant. I don't know. We can just think about that.

Emily Taylor: Kathy, did you want the mic?

Kathy Kleiman: I think we should go to WHOIS data. The WHOIS data is that of the agent and agent alone because domain registration data from a registry and registrar perspective is this. It's building data; it's a lot of other things. WHOIS data is smaller and it's our mandate.

Emily Taylor: Thank you. Nice point.

Lutz Donnerhacke: I'd like to thank that for a construct in which the registrant is acting. This implies that a proxy service is the registrant. That's fine. That's great.

Kathy Kleiman: If this is okay with the group, direction to Alice's change, "the domain registration data" to "the WHOIS data." Thank you everybody.

Emily Taylor: Thanks. That's good. So, we delete the previous one and do we adopt this one?

Kathy Kleiman: Here's to Seth.

Emily Taylor: Yeah, good job, Seth. Thank you. Thumbs up.

Kathy Kleiman: Privacy. And I recommend we go back and think about this as long as the concept is okay, unless you're not okay with that, Bill. I'm amenable to changes on this one. You could explain what we meant by it.

Emily Taylor: I think I understand what you mean by it and that's certainly the way that some privacy services operate, where they just don't have a name at all. Is the concept clear to everybody? By privacy, we mean the registrant's name and a subset of other information, possibly null set, but consistent across ICANN, which is one of the drums we've been banging in our discussions. Sarmad.

Sarmad Hussain: I think the main thing is ownership, not the name either, actually, right? So, in the first case, the ownership is with the second entity or legal entity, whereas in privacy, the ownership is with the person itself. So, that's really the difference and that probably should also be captured.

Emily Taylor: Some people in the industry sort of bridle at the term ownership in relation to domain names, but I think that we can take WHOIS meaning the identity of the registrant or the way that the registrant is. The fundamental difference between a proxy and a privacy is that the proxy is someone else and the privacy service, you don't see their address, but it's the registrant.

Wilfried Woeber: I don't want to reopen the question of whether it's only available to natural persons or to other organizations as well. The question here is actually what do we mean by the registrant's name?

Sorry, then I didn't get it completely, so my question is are we requiring here the name of a natural person, or…? Which my feeling would be that my answer would be yes, or are we fine with some phony Cat Brushing Association's representative in northern Maine?

Emily Taylor: Did you want the mic, Bill? You were just twitching. Sarmad, you wanted to come in.

Sarmad Hussain: So, just further on that ownership, name may actually be the person's name, but ownership will be, maybe, often institution or organization, if we are saying that privacy can be taken up by an organization as well, not just a natural person.

Kathy Kleiman: I thought we were specifying a field. The field has to be filled in, whether it's a corporation, whether it's an organization, we're not stipulating incorporation or not incorporation, it's the field. So, I'm going to go pull up the record and see what the field is called—the registrant name field. I'm just going to double check. I've looked at it a million times, but let me just double check again.

Emily Taylor: Okay. Lutz.

Lutz Donnerhacke: Let me become technical on a domain transfer. Please consider what happens if a domain is transferred from one registrar to another. What information do we need for a transfer? At least we need a name of the person who is initiating the transfer. We have to check if the person has the right to transfer the system or the domain. Does it affect this?

Then, in a few cases, an email is sent. Privacy service would prevent or relay it for a given time. No problem. So, the question arises if the real name of the person behind, or the organization name behind, a privacy service should be possible at all or not? Just for everyday operations in the domain, its name system.

Emily Taylor: I have text amendments. I don't want general discussion on this. I just want to get text amendment suggested, please. Kathy.

Kathy Kleiman: I know there is some variation. I'm looking at a network solutions record. I would put in, instead of registrant (apostrophe *S*'s) name, registrant (capital *R*), name (capital *N*), and make it clear to the group.

All these are broad definitions, so what we're doing is talking about the data that goes into that field. I think by identifying it, at

least the way I've seen it many times—I know there are some variations—so, registrant (no apostrophe *S*), name (capital *N*).

I think we're making it clear that, at least from our perspective—and again, this is all going to public comment, guys—that the quid pro quo for privacy service is that you publish registrant name.

Susan Kawaguchi: Somewhere in all of our discussions in the last year, we wanted the format to be standardized, so it's all going to change anyway, to your point.

Emily Taylor: Okay. Whole document—thumbs up or thumbs down? Peter.

Peter Nettlefold: We forgot the one that we forgot before that I've found in my wording.

Emily Taylor: Okay, let's go up to it, please. Can you tell us a relevant place in the document?

Peter Nettlefold: Yeah, in the conclusion, so just go on a little. It's right near the top of the conclusions and it will be between one and two. And the straw man is for the avoidance of doubt, comma, ICANN should

include an affirmative statement—this next bit might be in or out—in the RAA that clarifies that.

You'll notice when you use in the words in Seth's definition, which we're all happy with, that of proxy services, blah, blah, blah. That a proxy is a business relationship, dot, dot, dot, dot, dot.

I know there's at least one lawyer in the room who might have some better way of saying it than that, and I guess there's a question about where ICANN puts the statement, but it seems to me the clearest place would maybe be in the RAA.

I'm aware the two others may have a better understanding than me, but I think this will help clarify what we're trying to push forward here.

Bill Smith: I would suggest that that language would go into the policy document, not the contract, because then it could be referred to from multiple contracts or other places.

Emily Taylor: So, no, not the policy chapter and this. Instead of saying "in the RAA", rather than saying "ICANN should include an affirmative statement in the RAA," that you mean that the -

Bill Smith: I'm suggesting WHOIS policy, and then however they choose to affect that. Could be the RAA, could be in a document.

Emily Taylor: Clarifies that a proxy means… And that we delete "ICANN should include an affirmative statement in the RAA." That's what you're proposing? Wilfried.

Bill Smith: Should include an affirmative statement.

Seth Reiss: Just delete RAA.

Bill Smith: Exactly.

Emily Taylor: Sorry. We want the statement and we're happy with what that statement is, we just don't know quite where it should be. Unsurprising at this hour of the day. Wilfried, you had a comment.

Wilfried Woeber: Just a question of what the potential timelines involved would be. If it would take about as much time to modify the RAA as it would take time to come up with a policy, then I'm fine with that one.

In case we would expect that the policy development is taking much longer than it would take to modify the RAA, I would lean more towards the initial proposal to modify the RAA just in order to prevent the mess becoming bigger and bigger and bigger for another six or twelve months. I don't know what procedures would be involved to modify the RAA.

Emily Taylor: Kathy.

Kathy Kleiman: You also don't want to direct, necessarily, who's going to implement this. So, we don't want to go past the GNSO and say we're directing ICANN staff to do this directly. Let everybody come in, put their fingers on it, claim some ownership, but it's very clear what we want.

Emily Taylor: Currently, that sentence isn't making a whole lot of sense to me at the beginning. It's currently reading, "For the avoidance of doubt, ICANN should include an affirmative statement that the WHOIS policy clarifies that a proxy means a relationship," blah, blah, blah.

So, do we mean the WHOIS policy should include an affirmative statement, that? Bill, can you help me out on this? Because the sentence is currently having so many subordinate clauses, I think we're going to all die before we get to the end of it.

Kathy Kleiman: I thought it was just me.

Emily Taylor: And, is that what you mean?

Bill Smith: That. "An affirmative that clarifies." That.

Emily Taylor: Yeah?

Bill Smith: Yeah.

Emily Taylor: Are we in agreement on this, on these recommendations? Have we approved this document? Can we have a last thumbs up? Do we approve this document? I've got just puzzled looks from over that side of the table. Do we approve -

Lutz Donnerhacke: Just to overcome my limited English, "a registrant is acting on behalf of another." Another what? Registrant? Entity? Okay, that's fine.

Emily Taylor: Can I just ask again? Can we confirm that this document containing the findings and recommendations relating to proxy and privacy is approved? By consensus? Can we have some response from Bill and Lutz?

Bill Smith: You have rough consensus from me.

Emily Taylor: So, you can live with it?

Bill Smith: That's a different statement, okay?

Emily Taylor: Well, I don't need it chapter and verse, but what I need to know is do we have a set of recommendations that are agreed?

Bill Smith: Okay, I'm trying to be as specific and explicit as I can. By the IATF definition, I am not objecting and I believe we have rough consensus at this point, alright? I can't tell based on the status of the document right now what it actually is saying, but I am not objecting to anything that I know is in it.

Lutz Donnerhacke: Same to me from the other side of the…

Emily Taylor: Thank you, I think, Peter.

Peter Nettlefold: And I'll say thank you as well. It's pretty clear down this end of the table is where there has been a serious move towards compromise, and it may be that we have two people who are equally unhappy, so I genuinely thank you two.

Emily Taylor: Thanks again for all the work on that. That's been a hard slog, but we've done more than has been achieved on this in the last twelve years, so far. Famous last words. One thing I want to clarify for myself because if we need more time slogging these out -

Kathy Kleiman: Just a note from the chat room, we have a congratulations from Mark McFadden and applause from Michael.

Emily Taylor: Thank you. We had, I think, a set of WHOIS accuracy…this is the green stuff on page two of the NDR stuff.

Wilfried Woeber: Thank you, Michael.

Emily Taylor: I just wanted to leave here clear in my own mind of the status of these recommendations here. Can I just ask you to look at this piece of paper that I'm holding up, everybody in the room? It is. That's the third page and that's the second page. Bill.

These we spoke about in Marina Del Rey for about two days and we finally set these as green signifying that we agreed them. My confusion is that when we went through them yesterday, we were reopening it all. What do we want to do? Bill.

Bill Smith: My suggestion is if we had agreement, we have agreement. I don't know why we would reopen them?

Emily Taylor: I wouldn't want to do that and I was confused about it, but I justified it in my own mind as in fact we were discussing privacy and proxy, by proxy, because I don't think that we had any disagreement on these and that we were happy with them.

Kathy Kleiman: But, yesterday when we started looking at them, we began a series of edits.

Emily Taylor: But they were not substantive. Read them now in relationship to our work on privacy and proxy.

Kathy Kleiman: Okay, fair enough.

Emily Taylor: If we have any major comments on them I do not want to reopen these unless people have got absolute "I'm going to die in a ditch over this," okay? I want to say we have an agreed set of recommendations on accuracy; we have an agreed set of recommendations, albeit that we are all slightly or to some degree very unhappy we have an agreed set of recommendations on proxy/privacy. We also have what I would describe as pointers here in this brainstorming which need to be read alongside those that we have hammered out in detail, but I think we've covered proxy/privacy, we've covered accuracy. We have some wording on that target that we negotiated and worked through of reducing the number of unreachables which needs to be added into our accuracy ones. We've got the IDN policy and implementation that we need wording on from you.

Kathy Kleiman: Can we actually just read them one-by-one and go through without, and do the same thing – "In principle do we agree?" And

not wordsmith but "In principle do we agree?" because it's hard to see some of them.

Emily Taylor: Number one, accuracy: "ICANN should ensure that the requirement for accurate WHOIS data is widely and proactively communicated. As part of this, ICANN should ensure that its registrant rights and responsibilities document is proactively and prominently circulated to all new and renewing registrants." Come on guys, thumbs? Yep.

"ICANN should ensure that there is a clear and unambiguous enforceable chain of contractual agreements with registries, registrars and registrants to require the provision and maintenance of accurate WHOIS data. As part of this, ICANN should ensure that clear, enforceable and graduated sanctions apply to registries, registrars and registrants that do not comply with its WHOIS policies. These sanctions should include deregistration in cases of serious or serial noncompliance."

[background conversation]

Emily Taylor: No, we add a year on the WHOIS Review Team. Sarmad?

Sarmad Hussain: So I think we derailed here yesterday where we were saying "down to the registrants" rather than "the registrants." And so I'm just first of all pointing that context out, and I guess we all need to go and think and see whether what we added now addresses that or is it still of value to add "down to the registrants" here.

Emily Taylor: I think in my considered opinion I don't think it adds anything or changes the meaning. And I think that we got derailed yesterday because we were actually talking proxy/privacy and all of the issues around that which we've now to some extent cobbled together. Lutz?

Lutz Donnerhacke: What about resellers? I do not find resellers here.

Emily Taylor: I think, Lutz, if I can speak to that, resellers are dealt with in the RAA quite clearly on the basis that whatever the situation is the registrar maintains the responsibility. And that's actually what we're asking for here – we're asking for a clear line. And so the resellers-

Lutz Donnerhacke: That's okay. Thumbs up from me.

Emily Taylor: Okay, so thumbs up on that. Number three: "ICANN should take necessary measures and allocate sufficient resources to be proactive in enforcing its WHOIS policies and contracts. The ICANN community should develop a cost-effective and workable mechanism to proactively verify WHOIS data." Whoa! Sorry, I can't even read it – I'm reading this because I can't actually read anything that's on the screen. No, don't touch it – it's fine.

[background conversation]

Emily Taylor: Yes, we agreed these in Marina del Rey. I do wonder about this.

[background conversation]

Emily Taylor: Yes, I actually queried into my own mind. Can we park that? Can we just put this as yellow because I do think that this is a contentious one and I can't imagine that it's going to… I was surprised to see it here.

Kathy Kleiman: And I think that the concept is maybe the same, that the ICANN community should take steps to improve the contactabiltiy, the accuracy and contactability of the data. So let's not put this

down… The last one was approved, by the way, Alice, number three. But here, "proactively verify…"

Emily Taylor: Can I make a suggestion? We hammered out over half a day I think a very good, very achievable and workable solution on what we expect to see with data accuracy before the next WHOIS Review Team, and that is that those non-contactables are reduced down by 75%. And I would move that we substitute that in for #4 here.

Kathy Kleiman: Second.

Emily Taylor: You guys?

Peter Nettlefold; I will just quickly say that I drafted this and now that we have those great targets I'm happy to see it go if need be.

Emily Taylor: Wilfried?

Wilfried Woeber: Yeah, in favor of the proposal. Just to provide a little bit of history, if I remember correctly we had this longstanding

discussion that we should rather try to make sure that the registrant's data is correct at the time of registration. And there were lots of contributions like double checking with credit cards and those sorts of things.

I think the idea behind that was try to get it right at the very beginning instead of trying to fix it later on if I remember correctly. But that was my reading.

Seth Reiss: I just happen to like this recommendation but and I understand that we don't have a consensus on the point, and so I just wanted to be able to concede.

Emily Taylor: Thank you, Seth, so I think that we have agreement. If you can turn off your mic now, Seth, so that my mic is on – thank you. We have agreement to delete this and substitute the one that we wrote this time. This is the one about 50%, 50% - "ICANN should…" Oh God, I can't even see it.

Kathy Kleiman: Can we let Peter bring in the language?

Emily Taylor: "ICANN should take appropriate measures to reduce the number…" "ICANN should reduce the number of unreachable

registrations or take appropriate measures for easy targets, reduce the number of unreachable registrations…" this one. Yes? Just trying to get out the door in six minutes so that I don't miss my plane home, and that is my top priority at the moment.

Sarmad Hussain: So I'm happy to have that second recommendation brought in but I'd still suggest, this may be too strong – to dilute it a bit, but not throw it away. Because we're talking about two different things when we are talking about the accuracy of data coming in and the accuracy of data already in the system. And we do really need to look at both things.

And the cost of cleaning data while coming in is going to be much less in the longer term. That's what we normally study in engineering design as well – you know, to fix something which is badly designed later on is sometimes many fold more costly than having it designed properly at the outset. So we're talking about two different things.

You can perhaps dilute it but I would request that you may consider having some formal check so we can discuss what we want to put in. But have something on accuracy of data coming in.

Emily Taylor: Madame Chair, in the interest of time may I suggest that we take the number 4 in yellow and put "Not Approved" in large letters,

but we'll return for further discussion. And then we call the next one number 4 because it looks like we've agreed to the ICANN… Call that #4 and say that's, if we all approve it, then that's approved and then hopefully move on.

Emily Taylor: Peter, did you want to make a comment?

Peter Nettlefold: I was going to suggest some wording just to see if it would work off the cuff but-

Kathy Kleiman: Without James? I'd wait for James on this discussion.

Peter Nettlefold: Instead of "proactively verify" I expect is the sticking point in #4.

[background conversation]

Peter Nettlefold: Yeah, okay. Yeah, that's true, but we're really looking at a mechanism which provides some improvement or assurance. So yeah, okay, I'll let you go. We can talk about it later.

Emily Taylor: Okay, so I think let's… I think the way through on this is concepts like exploring through dialog and cooperation with registries and registrars, effective mechanisms to improve data accuracy on the point of registration but making the point that this is good but it's not a stick that is not in, you know, it's not thingie, I can't think of the word.

Kathy Kleiman: And just by way of background, in some countries it's easier than in other countries. Verification is a country-by-country, area-by-area.

Emil Taylor: Yeah. So we're going to revisit that one, the one that's just above that. We'll revisit that on the basis of thinking about that.

Kathy Kleiman: After "Not Approved" it says "Will revisit for…"

Sarmad Hussain: I'm a bit uncomfortable with "not approved." I think there's probably general agreement on this, so instead of "not approved" probably say "dilute or make less genera" or something like that, unless we're not approving it.

Emily Taylor: I actually hear from Kathy and I believe James would view that as difficult, but I don't think anybody in this whole Review Team would be against the idea of exploring ways to improve data accuracy at the point of registration.

Peter Nettlefold: James said it in Marina del Rey – it's the best stuff we can do.

Kathy Kleiman :That's different than an absolute requirement for complete verification which this can be read as. But I'm with you in principle but that language at this point is not good.

Emily Taylor: Okay. So scrolling down, oh, Sarmad?

Sarmad Hussain: Sure, but I still do not agree with "not approved." I'm happy with saying…

Emily Taylor: Okay, you're going to have to slug that out without me. I just want to get through to the end of this list and then I would ask you to stay on with Kathy chairing and then try and resolve that.

Okay, #4 we're happy with in principle because we are. The other #4 below that is "Building on the 2009 [NORC] study, ICANN

should commission regular studies to measure WHOIS accuracy. These studies should provide time series data to enable definitive assessment of ICANN's performance in improving WHOIS accuracy."

Bill Smith: I would ask for if I could, rather than "commission" that we "conduct."

Emily Taylor: I'm very comfortable with that and for the reasons we've discussed. Thumbs up.

"The results of the next accuracy study," can we say in #5? Yeah – that's fine. We're on #5 now. So "The results of the next…" please delete "ICANN-commissioned." "…accuracy study should be available for consideration by the next WHOIS Review Team." Thumbs up?

[background conversation]

Emily Taylor: Approved. "If a significant, measurable improvement in WHOIS accuracy is not demonstrated from one accuracy study to the next this should create a strong presumption that the ICANN Board will set aside additional and dedicated resources to increase its WHOIS

education, auditing and compliance activities." And then we've got #7…

Sarmad Hussain: The improvement, the lack of improvement could also be due to not appropriate policy, and that's not covered here. So we also need to revisit policy, not just compliance.

Emily Taylor: And bear in mind that we are asking them to revisit policy, yeah. Yeah. Okay. I think I'm going to have to really go now. We have one here which we were unable to reach consensus on in Marina del Rey. I think that's…

Kathy Kleiman: I think we should let you go and I'd like a standing ovation for Emily because I think she's done a stunning job for our three days.

[Applause]

Emily Taylor: Thank you very much.

Kathy Kleiman: Does anybody want to continue the discussion on #7?

Lutz Donnerhacke: No.

Kathy Kleiman: I think we're going to be here for a while.

[background conversation]

Kathy Kleiman: Okay, so let's say what we renumber and just get what's approved right.

Emily Taylor: Thank you all very much. I know it's been tough today and I know I've nearly lost it or possibly even lost it on a couple of occasions but I wanted to say thank you very, very much.

[End of Transcript]