BUENOS AIRES – EWG Workshop
Wednesday, November 20, 2013 – 16:30 to 17:30
ICANN – Buenos Aires, Argentina

UNIDENTIFIED MALE: Thanks, Fabricio. So, first of all, thank you very much for being with us this afternoon. I think it's great that a lot of people still get some energy to be with us after this busy day.

I think this is the first time that we have created this open space to create. And we have retained for this afternoon four domains, four areas where, I think, we would like to capture your creativity, your attention, and your insights.

So this is basically your space. We are inviting everyone to be as expressive as possible in such a way that we can incorporate your comments, or clarification, or whatever because we have also few people from the EWG also attending this session. So this is really a space for all of you to be challenging us and at the end hopefully more comfortable of what we have been put in to this status report posted last November 11.

With that, we have the data, we have the model over there, we have validation, gated access, and we have privacy, of course, just behind me. Do we want to split ourselves around these four whiteboards, and then I'm sure we can gather some staff people capable to record and to make sure that we keep track of everything which will be said.

UNIDENTIFIED MALE: Can't we just discuss it together?

UNIDENTIFIED MALE: You mean, discussing after that? Yeah. You can position yourself into a one, or you can turn, or you can.

UNIDENTIFIED MALE: Okay. He wants to talk to you about stuff.

UNIDENTIFIED MALE: You're a small enough group. I don't think. I don't know.

UNIDENTIFIED FEMALE: It's a small group.

UNIDENTIFIED MALE: Yeah. It's a small group. You could.

UNIDENTIFIED MALE: It's very small, yeah.

UNIDENTIFIED FEMALE: Would the facilitators of each group like to just remind people what the groups will be addressing, and then we can ask people to go to the respective groups?

UNIDENTIFIED FEMALE: Or, what's easier? If there's a small group, you want to stay and discuss.

UNIDENTIFIED FEMALE: Oh, sure.

UNIDENTIFIED FEMALE: I think we wanted the dynamic of the small groups.

UNIDENTIFIED FEMALE: That's true.

UNIDENTIFIED FEMALE: Oh, this is a small group.

UNIDENTIFIED MALE: We have an hour. We want to go an hour.

UNIDENTIFIED FEMALE: There is a problem that the groups will be so small that there's no dynamic. I would hate to be the only wallflower with nobody coming to my session, you know?

UNIDENTIFIED MALE: Also, ICANN staff, is there a reason why the microphones are all flashing?

UNIDENTIFIED FEMALE: Yeah.

UNIDENTIFIED MALE: Because I touched one; thank you. Because I guess I touched it.

So if we're going to do that, well, why don't we just put the board right here in the middle – each board or just one – and just put "privacy" and talk about privacy, and put another one up and we just split it up and everyone can get their feedback into it. Then you get one or two scribes, and then run the hour that way.

UNIDENTIFIED MALE: It would be comfortable that we risk that because we're going to start with some, let's say privacy or data or whatever, then we are not going to finish in one hour.

UNIDENTIFIED MALE: So, why don't we do this. If we have an hour, split it up evenly, and if people feel passionately after the moment has stopped for, say, privacy, the board moves over and you can continue or move onto the next subject.

UNIDENTIFIED MALE: Exactly, very good.

UNIDENTIFIED MALE: Sound good?

UNIDENTIFIED FEMALE: So we start with privacy.

UNIDENTIFIED MALE: So we start with what?

UNIDENTIFIED FEMALE: Privacy.

UNIDENTIFIED MALE: Privacy?

UNIDENTIFIED FEMALE: Wouldn't it make more sense to start with data elements? Because then we'd understand what privacy meant.

[crosstalk]

MARGIE MILAM: For those who have wandered in, please have a seat. This is going to be a very interactive session. Yeah. Can we turn this off?

[crosstalk]

MARGIE MILAM: Just a quick technical announcement. For those who are joining remotely, you'll need to get into the Adobe chat room on your

computers. We'll enter information in there so you can participate through the Adobe chat room.

UNIDENTIFIED MALE: Hey, if I pulled a muscle carrying that over here, can I file for some sort of Workers' Comp?

MARGIE MILAM: Absolutely.

[crosstalk]

UNIDENTIFIED MALE: Yeah, there's a lot bad going on here.

UNIDENTIFIED FEMALE: Okay, I'm not the only data person, so we can all.

UNIDENTIFIED FEMALE: Yeah.

UNIDENTIFIED FEMALE: Hello?

[crosstalk]

SUSAN KAWAGUCHI: Okay, so if we're starting with data. Hi, I'm Susan from Facebook, and I've been part of the WHOIS review team and then signed on for the EWG. So it's an interesting experience with WHOIS or new data records for domain names.

We just have a limited number of handouts, but I think it's really important, I think for myself at least, in viewing this as not a part of the EWG to know what our thinking is on what's going to be in the data record, what we're proposing at this moment at least.

We have a handout there. I think page 63 is probably going to be your most interesting page because this is the minimum anonymous query response. So if I want to know what example.com I think is the domain name, or example.tld, where I can anonymously pull the public data – so I don't have to do any validation, no log-in, no nothing – this is the data you'll get.

All of the registry data, all of the registrar data, but a very, very minute data elements from the registrant. And I know, Steve, you brought that up as you were, I can't remember how you put it, shocked? That's that what we came up with for the anonymous.

In looking at that, is there a discussion around that?

PETE ROMAN: I have a question.

SUSAN KAWAGUCHI: Oh, I'm sorry.

PETE ROMAN: She's like looking around, so I was waiting until she could see me. Hi, Pete Roman, U.S. Department of Justice.

My question is my memory of how WHOIS got started was that we were all trying to have contact information in case something went wrong, and the one thing you've completely excluded from the public access stuff is all the contact information.

SUSAN KAWAGUCHI: Well, it…

PETE ROMAN: Right? It's all here in gray at the bottom of page 62, and none of it's showing up in the public stuff. So if I'm just your random sysadmin and I have a problem and I want to contact the guy whose site keeps pinging me, I have to go to the registrar before I can actually go contact the guy?

SUSAN KAWAGUCHI: So now if you look at the bottom of page 64, actually. I may have. Where is it? No, 63, excuse me. If you look at the bottom of that, you're going to get the domain name. You'll get the name servers, the name servers will give you some sort of information. You'll get the registrant type. And then you will get a registrant contact ID and the registrant e-mail address.

We had quite a discussion on what do you need to take care of a technical issue, and the e-mail address is what we decided was probably the most important.

PETE ROMAN: Why are you giving out the registrant's e-mail, which might be really only intended for the registrar, as opposed to giving out the registrant's contact e-mail, which was clearly intended to be used to contact him?

SUSAN KAWAGUCHI: I guess I'm missing the distinction.

UNIDENTIFIED MALE: I think it is the registrant e-mail, actually, the bottom of page 63.

PETE ROMAN: No. It says "registrant e-mail," but there's also a contact e-mail on the bottom of page 62 in the contacts that we are not sharing as the contact e-mail, which when I was doing this was the contact e-mail that I wanted you to contact me at. The registrant e-mail was the contact info that I wanted the registrar to contact me at.

So why am I sharing the stuff that I want the registrar to use with the whole world and not sharing the stuff that I want the whole world to use with the whole world?

SUSAN KAWAGUCHI: I would think we intended that this is the e-mail address that you would want anyone to contact you at, and there's also…

PETE ROMAN: Then, why not use the contact e-mail?

MARGIE MILAM: Can I jump in here? I think you have to use the contact info because the other e-mail's protected under data protection legislation, so it's the contact info.

PETE ROMAN: But then if this is the contact info, you should probably fix it so it says it's the contact info.

SUSAN KAWAGUCHI: I think maybe what is lost when you just look at the example sort of absent the description behind it is that there's the concept of having role-based contacts. The particular example you're looking at, the registrant is an individual and didn't provide role-based contacts, so the only thing you have is the registrant's e-mail address.

We would think that the normal case would be that registrants would choose to provide a technical contact and an administrative contact, and they would default to public. They could, registrants could provide that information and ask that it be private – gated, if you will – but that

if chose to provide it by default, it would be public, particularly to enable contact as you say.

For example, in my own domain management, I would put everything public, and I'd have that option. But for our company, the registrant, the administrative contact, and technical contact is all the same, so there's no need to actually address all those roles. It's like if you want to know, here's the phone number, here's the domain@facebook.com and that comes to me. I then hand it out or there are other people looking at domain@facebook.com.

We do envision that companies may have a different burden put on them, but this is just simply for an individual. This is going to be the lightest weight of public access information you receive. Yes?

JAY DALEY: Thank you. I don't actually agree with our friend over there.

SUSAN KAWAGUCHI: Could give your name, please?

JAY DALEY: Yes, sorry. Jay Daley, from .nz. I think one of the problems we've always had is people misunderstanding the difference between the registrant details and the contact details. To me, the registrant details are not the contractual issue between the registrar and the registrant; they are the authoritative record for the registry.

Every registrar I know would have a different set of data about their relationship with the customer, and it's not going to bleed into this at all because they don't want it to. So the registrant is the right thing to have here, as I understand it, in that type of way.

The thing that I find slightly odd is the lack of address detail, postal details there because the implication is then that if you want to send somebody a formal notice like a cease-and-desist letter or something like that, you then have to use gated access for it.

SUSAN KAWAGUCHI: Right.

JAY DALEY: And I believe that pushing you into gated access for that is not necessary, you know?

SUSAN KAWAGUCHI: Michele?

MICHELE NEYLON: Jay, just this entire thing around public and gated, I think a lot of you may be laboring under the perception that "gated" automatically infers high-level of validation of the person requesting access to data. That's not necessarily the case.

As most of you probably know, you do a WHOIS lookup from a command line WHOIS client. You're not really sharing any of your own

information. I mean, you have a certain degree of anonymity. Depending on the WHOIS server you hit up against, it may get an IP address, it may not.

With the kind of lighter form of gating, it could simply be a question of you going to a Web form, maybe you might need to authenticate with something but at a very, very light level, not a case of, you know, I don't know, send in a blood sample and a copy of your driver's license and a check for $100,000 or anything. It's just a case of "we" will get more information about you but not necessarily a huge amount.

SUSAN KAWAGUCHI: Right.

JAY DALEY: If you're going to specify that, and you're going to say, "Right, this is the level of gating that's required to get access to that," and that's then going to be properly policed afterwards, then I could probably live with that. Okay?

UNIDENTIFIED MALE: That will be up next.

JAY DALEY: But it sounds to me as though that gating there that you've just that described, you enter a CAPTCHA or something like that, is actually just about controlling people taking too much data, looking up too many

things, and that doesn't need to be done at the client end. You can do that at the server end.

SUSAN KAWAGUCHI: Well, we haven't really come to terms with what that gate is yet, or what the access to get through the gate is, to be honest. So I think at this point we would have varying opinions on that, but letting us know what you think would be good for the validation would be interesting.

Was there a gentleman over here?

FABRICIO VAYRA: Yeah, I was just going to say the basic premise we're having here is that if Joe Blow Consumer wants to just quickly check, "Is this a person, a company?" wants to write an e-mail, "Hey, did you know your website is down or something bad is going on?" what registrar you are, kind of system-generated data, that's not highly sensitive information. So if you just want to have a quick talk with somebody.

But if you want to get beyond that, like a home address or something like that, as Michele was saying, there just needs to be an extra level so that we know that you're not just kind of randomly seeing things that you could misuse without giving anything about yourself.

So in my instance, to send a cease-and-desist letter, if the rules are set up, I'd be more than happy to send it via e-mail, especially if it's known that that e-mail's tied to – if you don't answer, or you don't do anything, or it's invalid, or it bounces – it's also tied to the RA.

But I also would have no problem doing something like Michele said, where I do want the address. I have no problem saying, "Hi, I'm Fabricio, lawyer for Time-Warner, and I'm going to send you a letter. Give me that info."

But I do think that you're hitting right on the spot. I think that there's a balancing act here on the validation, and I think that's probably what was getting to Steve earlier as well is there is a danger that that can over-rotate in a wrong way, and we need to just strike the balance on that.

JAY DALEY: Can I just say, then, that I think that the registrant type should determine the default public data that is provided, then? Because a legal person is very different from a company in that regard and publishing a company's address.

SUSAN KAWAGUCHI: Right.

FABRICIO VAYRA: Correct.

JAY DALEY: My understanding of my data and my registry is that it is largely corporate addresses and organizational addresses. And I think that

that's the way that people use WHOIS data a lot is for those organizational addresses.

FABRICIO VAYRA: We agreed with you, and actually we had a full discussion – almost days – between how you could do commercial, non-commercial, corporate or not corporate.

One of the things we actually discussed was explaining very explicitly as you go through the registration flow, "This is kind of your basic data that will go out. This is the stuff you fill in. And by the way, there'll be a way that you can check and say make this all public." And then why is it a benefit of this? And we would actually say, "As a company, you may want to actually show all this information so people know exactly who they're dealing with and can contact you, etc., etc."

SUSAN KAWAGUCHI: But we also could decide that as a company, you do not have the rights that an individual does anywhere.

JAY DALEY: That's the point, I think, you very much need to make [that you don't].

SUSAN KAWAGUCHI: Therefore you will once we, you know, I've talked about a bright line in the past. You've stepped over that bright line to, yes, you are a commercial enterprise of some sort. You may be acting in your own

name doing that, but by doing that then your address and other data elements will be shown.

JAY DALEY: Because of consumer protection effectively.

SUSAN KAWAGUCHI: Right.

JAY DALEY: Yeah, I agree with you.

MARGIE MILAM: I'm conscious of the time and the other three areas, so if we could quickly hear from people who are not on the working group, and then we're going to have to…

SUSAN KAWAGUCHI: Okay. I'm sorry.

MARGIE MILAM: No. It's been a really useful discussion. I think Michael was…

[MICHAEL]: Was I?

MARGIE MILAM: Yeah.

[MICHAEL]: Okay, thanks. I would agree with mostly everything that Jay had just articulated with regard to the concerns and then after hearing what you said addressing some of those fears.

My suggestion to the working group if you want to conclude your three-month volunteer service hopefully by Singapore, perhaps if you could articulate in the near future what that gating would look like.

Because with not knowing what that gating function is going to look like, if this is the complexity of signing up for, say, a Google Gmail account or a Facebook page, something that can be that simple, I think that would go a long way towards addressing the fears as Michele or Steve was articulating. That will help, I think, further focus the work and the comments and allow you guys to finish up.

MARGIE MILAM: I absolutely agree with you. Steve?

STEVE METALITZ: Yeah. My question really was about this example on page 63 is a registration by a legal person, and I thought you said that the rules would be different for registrations by legal persons? But this is the one that we were raising the question.

SUSAN KAWAGUCHI: Yeah, that's a little confusing to me, too in that. Lisa can…

LISA PHIFER: Actually, we have a comment from the chat that we need to introduce.

SUSAN KAWAGUCHI: Oh, okay.

LISA PHIFER: Sorry.

SUSAN KAWAGUCHI: So I am viewing this, and this is something we've sort of, that that's an individual.

STEVE METALITZ: Okay. Well, I do have a question about how that data element will be validated. I don't know if this is the appropriate time to raise that.

SUSAN KAWAGUCHI: An individual?

STEVE METALITZ: Registrant type.

SUSAN KAWAGUCHI: Yes, we haven't gone there.

STEVE METALITZ: Okay.

SUSAN KAWAGUCHI: You know, I mean, I'm sorry for not having all the answers, but it's…

UNIDENTIFIED MALE: A long discussion.

STEVE METALITZ: I would suggest this is going to be the most difficult data element of all to evaluate.

SUSAN KAWAGUCHI: I would agree.

STEVE METALITZ: I think you should seriously consider whether your need this data element because it's a big validation.

SUSAN KAWAGUCHI: We've also thought about self-selecting. There was a comment over here.

TIM CHEN: Tim Chen from DomainTools. Just on the data, the original registration date is optional. Gray elements are optional to collect. So are you saying that there may not be the original registration date listed in the WHOIS record anymore?

SUSAN KAWAGUCHI: No. The creation date would always be in the record. The original creation date was something that I use extensively in my work day-to-day. The original creation date may have been, say, a domain was registered in 2000, deleted in 2002, and created again in 2003. It's very helpful to know that it was registered in 2000 to start or maybe it was registered every two years because it just deletes and continues to be picked up again.

That's just so the original creation date is something you can get a WHOIS history. Michael did point out today in the earlier session that that's not always accurate because of some transition issues early on.

TIM CHEN: Okay, so just something clear, that may not be if the registrar can choose not to make that, or the registrant maybe? I guess it must be the registrant. The registrant's not going to know that, right?

SUSAN KAWAGUCHI: Yeah.

TIM CHEN: So this has to come from the system.

SUSAN KAWAGUCHI: Right, and it may not be available even, or it doesn't exist, because the creation and the original creation date was… Okay. I think we have somebody in the…

[ALICE JOHNSON]: This is [Alice Johnson] voicing Kathy Kleiman's comment Adobe Connect Room. "Many legal persons are protected in many countries, including minority groups, political groups, religious groups, often incorporated."

SUSAN KAWAGUCHI:: And I think that goes to the local jurisdictions, that discussion.

MICHELE NEYLON: Just one thing. Some of the stuff we're not 100% locked down on, this is why we're having these conversations. Because we know, I mean how can I put this? We know that what's currently there is not helping a lot of people. Nobody's particularly happy with us. Whether you're a registrar, registrant, registry, law enforcement brand, privacy advocate, whatever – you've all got issues with us.

The sum complexities like the jurisdictional thing is one which is causing us massive headaches, the gating, the registrant type. I mean, we're not 100% sure what the best way is to deal with some of these things, so

we're looking for the feedback. We're trying to get some input from people, so the contribution from Jay, that's really helpful.

SUSAN KAWAGUCHI: Yep, pick us apart.

MARGIE MILAM: May I suggest, since we're approaching 5:00 that we take one more comment on this, and then I think a natural segue is validation and gated access.

And I want to remind people who've wandered in late, this is an interactive session so feel free to join us at the table here and share your perspective.

Also, we don't actually have a hard stop and there's nothing else scheduled in this room, so we're happy to hang out longer and talk this evening, if you'd like.

SUSAN KAWAGUCHI: Is there another question on this side? Yeah, okay. Sorry, stepped on you there.

JIM GALVIN: I have a slightly different question to ask about data elements. I'm sitting here looking and seeing the examples. I'm wondering if the working group is going to speak to the issue of translating data or transliterating the data elements at all.

One thing that I would call out is I'm remembering back two years ago, the Internationalized Registration Data Working Group had made the statement that a registrant should not be expected to use anything other than their own local language or script.

Then of course, in all of these nice display examples here, it then begs the question of, well, what happens between whatever form it comes in? Will you speak to that question and affirm that recommendation or say something different? And then will you speak to, what happens on the display side? Should I take whatever's in, or should I plan to be doing something else?

SUSAN KAWAGUCHI: Don't think we've covered that completely.

MARGIE MILAM: If I may?

SUSAN KAWAGUCHI: Yes.

MARGIE MILAM: Scott Hollenbeck from VeriSign who is also quite active in the IETF WEIRDS group addressing this effort has, along with ICANN staff Steve Shang, has briefed the Expert Working Group a few times, and we have incorporated some discussion into our work.

Obviously, though, we aren't there yet. And I think one of the outstanding issues the group needs to discuss further is to what extent and how we're going to incorporate that work in the final report, which we're targeting for release around the Singapore meeting next March/April.

JIM GALVIN: If I may, then, just for completeness. There are, obviously, two other working groups that would feed into the answering those questions. There's the Expert Working Group looking at the requirements for internationalized registration data, which is supposed to also specify a data model for the data, so there's a relationship there in that.

And then, of course, the GNSO. I haven't actually checked their agenda today, but in theory they approved a working group – and I'm getting some nodding heads, so they did – on asking the questions that had been put forth again by the IRD working group from two years ago about translation and transliteration. The specific questions are: Will there be a common language? And if there's to be translation or transliteration, who should do it?

So those are things to keep in mind, and I'd very much like for this group to consider and say something about this issue in your final report. That would be very much appreciated. Thank you.

UNIDENTIFIED MALE: I'm just going to read something from remote for Scott. Lisa website going to. Whatever. Scott Hollenbeck on remote is just saying that

"RDAP can certainly accommodate both localized and ASCII-only representations."

JIM GALVIN: Right. My concern is not about the protocol that's under development in WEIRD, since I'm sure Scott very well knows it's more about what the rest of the system is going to do. Because the WEIRDS, the RDAP protocol and WEIRDS behind it will take care of whatever's on the back end. Thank you.

ROD RASMUSSEN: Okay. Rod Rasmussen, another EWG member. I'm going to talk about validation and gated access, which the gated access we've already been talking about, so I think we can get most of that pretty quick.

And on that last point that Jim was raising, I think we have talked about this a bit. I think in general, although we haven't really gotten down to it yet, but in general, that's going to fall under one of those principles that we're going to suggest that the model and the way that the system is configured and policies around it conform kind of with whatever the other policies that come out of those other groups are.

We don't want to try and boil the whole ocean around all the other sub-policies on this, but that is an important point as to what are you going to display and all that from various international formats.

On the validation, I'm going to hold the validation for a second because we've been talking about gated access a bit. Gated access and the data elements go hand-in-hand, and it's hard to extricate those two different

areas because the gated access implies that some data elements are available under some rules apply to getting those and others they don't.

I think that in our conversations, we're envisioning what I would call three layers. One is the public, anonymous, anybody can look at it any time. All there is is some auditing around numbers of requests that are coming in. There's this idea of a lightweight, light form of access, where basically you're providing information about yourself as a requestor, but there's not an accreditation needed to get that level of data. And then there's a third level, which would be the highly sensitive data, depending on which buckets those fall into.

And that's obviously where we get feedback on from the community, as well, because we're trying to figure out what levels are what, where you would need some sort of credentials and validation of those credentials in order to get an accreditation of some sort. So that's kind of the three-tier model, if you can think of it that way.

Also, would note that on this there is certainly the possibility – in fact, it's going to be required – for automation of being able to pull data. I had a couple of people talk to me in the last couple of days about "I'm looking up 50,000 domain names a day because that's how many fake pharma sites that are out there, and we need to figure out what's going with them." There's way more than that probably even registered per day just for illicit pharmacies.

So you would have some sort of keying or some sort of automation that would allow for that. I know that's been a question a couple people have asked, so I figured I'd throw that out there as part of this process.

Looking for the other side of the gated access point is actually providing some sort of credentialing system, some sort of access system for being able to get at that.

If we had comments on that, and then I want to talk about the validation scheme, which gets into the content management part of it. But I want to get the gated access stuff out of the way, first. Jay?

JAY DALEY: Thank you. I think in the gated access, it would be good for you to remember that data is currency and that if anybody is asking someone for data that can be separated from the idea of credentials, then they're effectively asking you to pay.

And so it would be nice if there were fairly strict limits on what could be asked for, for the purpose of providing credentials and validation rather than just a data harvesting exercise.

ROD RASMUSSEN: What exercise?

JAY DALEY: Sorry. Data harvesting exercise.

ROD RASMUSSEN: Okay, right, got it. That's really kind of a terms-of-use, etc., or terms-of-reuse, etc.

JAY DALEY: Yeah. It's the terms under which people provide gated access so that they're not using it for much more than they should be using it for.

ROD RASMUSSEN: Right. Okay. And that goes right under our principles of purpose-based, purpose-driven.

And obviously, you need a compliance regime around that of some sort if you have people abusing their access privileges to get through the gate to get information. If they're turning around and doing something that's not the purpose, there needs to be some sort of a compliance around that.

JAY DALEY: Yeah. I'm talking about the people who run the gate, that they shouldn't be abusing their position in running the gate by asking for more data than they need for the purpose, very narrow, specific purpose of doing that.

ROD RASMUSSEN: Right, okay, yeah, got it. For providing it or whatever, depending on the model. Right, okay. I'm supposed to write this down, okay. Okay, any other comments on the gated access side of this? Or questions or thoughts? Steve?

STEVE METALITZ: I'm still having a little trouble understanding if the step up to gated access – in other words, to getting the credential – is very minimal, then what is the significance, really, of having such a limited set of data for the general public?

If the step up is very high, then I think that this is what people have a concern about. I'm sort of hearing different things about how high. And Jay's point, too, that maybe it will be exploited in other ways, but I guess I'm just agreeing with those who said it is important to try to pin this down a little bit because it helps to put some of the rest of it in perspective.

ROD RASMUSSEN: Yeah, and as I was talking about, it's not just one step but potentially two steps, right? There's a low step and then a higher step, depending on that. Okay?

I'm not sure who was first. Wendy or Stephanie. Wendy? She's not on the group, so she we should get her. Yeah, exactly. Yeah, okay.

WENDY SELTZER: Thanks. I was just wondering whether you considered sort of symmetries in the types of error that could be made. You've got inaccuracy in providing data as a registrant. You've got inaccuracy in providing data as a requestor of entry through the gate. Are there similar penalties for those who make the errors or willful inaccuracies and similar liabilities on those who allow them to do that, and in which ways do those errors sort of trend?

ROD RASMUSSEN: Right. That's important and, yeah, we have been thinking about it. We haven't figured out what the scale looks like yet though, right? But certainly that's part of our discussions and part of the work going forward. Was there input from . . . ?

UNIDENTIFIED FEMALE: Yeah. We have a comment here from Kathy Kleiman about gated access and shouldn't there be multiple gates or tiers of access, depending on the sensitivity of the data. And I believe that actually is the proposal.

ROD RASMUSSEN: Yeah, yes, and it's…

STEPHANIE PERRIN: Can I jump in here, Rod? That was basically the point I was going to make is it's important to clarify that "gate" is kind of the wrong word. Nobody likes "tier," but "gate" implies like there's a gate into a fairground.

In actual fact, what you're really doing is figuring out the purpose for which you're restricting different fields of data. There are a lot of purposes there: it's to stop bulk harvesting, it's to stop abuse, it's to protect personal information, it's to protect sensitive information, yada-yada-yada.

ROD RASMUSSEN: Jay?

JAY DALEY: Thank you. I think it's also important for you to remember that this is the Internet and not the subset of it called the Web. Okay? So I gate access to our WHOIS, always have done. It's called "rate limiting" and "whitelisting." The purpose for doing that is to prevent bulk data extraction. And so we mustn't always think it's a Web form and that type of thing. There are plenty of other ways to do it.

ROD RASMUSSEN: Yeah, that's actually been one of my big points that I've been making all along. I look at most access as going to be on an automated basis, when you look at just the sheer number of lookups. But it has to be, then, with some sort of purpose and some sort of credentials and all that kind of stuff, depending on what it is.

UNIDENTIFIED MALE: Thoughts on that?

ROD RASMUSSEN: You can put, sure. Sorry. Well, that was about it's not just the Web for getting data.

JAY DALEY: Okay. Sorry, Rod. Just to say, for us, the credentials we need at some times is just an IP address. That's the very minimum set of credentials,

and it's a simple one. And I just think we don't need to over-engineer the credentials required sometimes.

ROD RASMUSSEN: Okay. Yeah?

MICHELE NEYLON: Jay, that's one of the things that we've agreed on, as well. It's a bit like that idea of the "cost." It doesn't have to be economic. It's just you give us a bit of your data in return for us giving you access to data.

UNIDENTIFIED FEMALE: If I could just add one comment building on what Stephanie **said** and whether "gate" is the right word. I think, actually, that badge that gets you through "gate" is the analogy that we've used a few times in the EWG. The badge identifies who you are in certain respects and also possibly identifies where you can go once you get through the big entrance gate.

Then you're looking at the individual data elements, the individual areas that you're able to go to. And what you went through to get the badge, to some extent determines the level of clearance once you get through the gate.

ROD RASMUSSEN: Steve?

STEVE METALITZ: I guess this raises just a general question about how we should read the status report. I do recall the tiered access (although no one wanted to call it that) concept in the original report.

I don't see it in this status report. Every example that's given suggests a binary system, I think. You have two examples. You have the one on page 64 of what the public gets, and you have one what the authenticated user gets. So I see two examples. I don't think there's any reference.

Anyway, my question is: Should we be assuming that anything that isn't addressed or contradicted by the status report that was in your initial report remains valid? I'm just trying to put these pieces together so we understand what the whole picture looks like.

ROD RASMUSSEN: Yeah, I think so. Yeah? Anybody disagree on the group with that? Okay, yes. I mean, there could be a gray area here and there, but, I think, for the most part.

MICHELE NEYLON: The thing is, what we've tried to do in the update is to go into more detail about elements that people said we'd glossed over in the initial report and to give you a better understanding of how we came up with what we came up with.

Because the reality is that most members of the group have spent, I mean, I don't know how many hours at this stage. I mean, we've had multiple face-to-face meetings. We've had two-day meetings that

actually became four-day meetings. We've had multiple phone calls. I don't know how many hundred e-mails have been swapped. There's been subgroup calls, sub-subgroup calls. There's been dinners where you pushed the plates to one side. You know? It goes on.

ROD RASMUSSEN: Yeah. Move along.

MICHELE NEYLON: So, we're not, stuff is not set in stone.

ROD RASMUSSEN: We're reliving it right now.

UNIDENTIFIED FEMALE: This is to voice a comment from Kathy Kleiman, "Can you talk about the difference of access for two specific groups, e.g. intellectual property and law enforcement?"

ROD RASMUSSEN: We are envisioning having credentials or access be differentiated for those two communities. The exact data elements that each would get, under which circumstances, haven't been nailed down. But we would look at those as different accreditation schemes and potentially different levels of access of information because you may not need the same data elements in order to do an intellectual property type of

action versus a law enforcement sort of action. The exact differences, that's what we're debating, and if you have input into that, that's great.

UNIDENTIFIED FEMALE: Well, actually, she made that comment.

[KAREN]: Hi, this is Karen from MarkMonitor. I think that those questions, while all really interesting and very important, are super-premature at this point.

I think that the Expert Working Group as far as I know – and you guys have been working for a lot longer than 90 days from February – was to present kind of a framework through which we were supposed to then discuss this as a community, through the policy development process and through the implementation process.5

Those kinds of details, I think, very much belong in the hands of the ICANN community through a structured discussion in the PDP process, which we're improving through a PDP process. But I think that this will all be shaken out and it shouldn't just be coming from the Expert Working Group, although obviously your input is extremely valuable through that, as well. Thanks.

ROD RASMUSSEN: That raises an important just overall, this is for all aspects of what we're doing, and that's very true.

What we're trying to do is, though, make sure that we provide enough details so that the PDP doesn't get bogged down in some of the areas it has before, so some guidance there. And yeah, we know that not everything that we suggest is going to get adopted. We'll live. It's okay.

But at the same time, we want to try and try to get as far as we can along the process to give you as much input from our coalescing and working as long as we have on it to come up with some things that would work. Peter, you had your hand up for quite a while.

PETE ROMAN: Thanks. One of the things that – and we've talked about it, and I talked about this earlier – that law enforcement would be concerned with the gated access is the possibility of tracking what we're doing. Law enforcement in general would prefer that we not be tracked pretty much in any way.

There are issues there not just with what you guys learn about our investigations but the possibility that somebody, a bad guy gains access to it and now suddenly knows everybody that we're investigating, how that investigation is going, who we've talked to, who we're looking at.

I don't know what your plan is, in terms of tracking. I know there's discussion about being able to audit users' access and what they do with it, and whether they're using it legitimately. I understand that, and I can see why you would to do that. But I have to say that we on this end would be really concerned if you're keeping lots and lots of very specific information about what it is that we're doing. This is the exact same conversation I had with the DomainTools guys earlier, too.

UNIDENTIFIED FEMALE: Can I respond to that? That's a well-known problem in data protection legislation and so, in my view, it would be easy enough to codify which types of requests require secrecy and which ones don't.

How you do that, technically, I'm over to Rod. But I think with proper consultation, that's an easy enough problem to fix. I don't think that you're suggesting that the dogcatcher's entitled to secrecy.

[ALICE JOHNSON]: This is to read a comment from [Monica] in the Adobe Connect room. "How could jurisdictions, governments agree on who should have access to what level of data under which conditions? Do you think you can find a global solution? Why not focus on connection via WHOIS for technical problems, and leave all the storage and access stuff to the different jurisdictions?"

ROD RASMUSSEN: Duly noted, I guess. Thank you. That's [good] input. Tim?

TIM CHEN: Rod, I apologize. I have not read the entire 84-page document, although I hear it's outstanding and I will.

ROD RASMUSSEN: Come on, catch up!

TIM CHEN: Yeah, so I apologize. And believe it or not, I've not been to all the WHOIS meetings either so if this has been asked, then I apologize. Has there been discussion about higher-volume access to the data? Because some of the information in WHOIS is useful only if you do more than one-at-a-time lookups.

ROD RASMUSSEN: Yes, actually, I was just addressing that a few minutes ago.

TIM CHEN: You were, okay. I'm sorry. I missed that.

ROD RASMUSSEN: Yeah, no, no worries. We fully envisioned the bulk of them if you count the most number of lookups would probably be automated, so the credentials are needed to reflect that.

TIM CHEN: From within the gated environment.

ROD RASMUSSEN: Yeah.

TIM CHEN: Okay.

[ALICE JOHNSON]: This is to read two comments that we received in the Adobe Connect room. The first one is from John Horton. "Thanks a lot to the Expert Working Group for the hard work you've put in on this issue, and sorry that I cannot be there in person. I'm interested in the Expert Working Group's thoughts on a couple of questions that relate to general principles as opposed to implementation details.

"First pertains to what I think is a presumption that anonymous access to WHOIS needs leads to mining and abusing, quoting from the PowerPoint. Is that based on any empirical data, or is that more anecdotal in nature?

"I'd be interested in better understanding the extent to which bulk data extraction for abusive purposes has been documented and what those abuses have concretely been.

"Second, has there been any discussion about balancing out a registrants' right to privacy and Internet users' right to know who operates the website, where the registrant is located, and so forth?

"Put a different way: Do folks on the Expert Working Group feel that Internet users have a right to know who has registered a domain name, or is there no such right?" Thanks.

Second comment is from Kathy Kleiman. "Could we hear more about the privacy…?"

UNIDENTIFIED MALE: Hold on, hold on, hold on.

ROD RASMUSSEN: The second point, yes is the quick answer.

MICHELE NEYLON: I'll speak very briefly, to John. Hi, John. The bulk anonymous access to WHOIS definitely does lead to mining. We've had multiple incidents reported to us where a domain name that was registered on, say, a Friday using a specially-created e-mail address and the registrant starts getting spammed within, you know, 48-72 hours.

In some cases, the spams are actually pretty vicious. We're talking about fake renewal notices, phishing attacks, all that kind of thing. But it's not purely anecdotal, and I know work has been done. Maybe Lisa or others might better speak to that.

UNIDENTIFIED FEMALE: Yeah, but if I could just mention very shortly the results of the WHOIS misuse study, which has been underway for forever, will come out and they found very strong correlation between anti-harvesting mechanisms that they tested and the level of misuse.

ROD RASMUSSEN: And we may or may not have been privy to that some of that data to inform our decisions here. We're running way behind. So you have one more comment?

[ALICE JOHNSON]: Can I jump back to Kathy's question? Kathy Kleiman's question was "Could we hear more about the privacy and jurisdictional issues that are being debated?"

ROD RASMUSSEN: Okay, well, that will be under the "privacy" area.

UNIDENTIFIED MALE: That's up next.

ROD RASMUSSEN: Yeah, that's up next, and so if we get that board up here. My own pet project is the whole validation stuff, which we didn't really get to. And that's around what I would really like people to comment on and come give us input or track me down to talk about this concept of individuals or individual organizations having control over their contact information and really creating, if you take a look at what we're proposing here, almost a parallel system where you're actually registering contact data separately from domain name registrations.

So you have the concept of you as an individual or as an organization control your information, update your information using a validator of some sort that then is tied to domain name registrations. That's a really important, big concept. It's a big change we're talking about here, potentially, on how this is managed.

Now, the good news is the EBP and everything was set up to do that because way back in the day, that's actually how it was managed. And so the back-end systems can actually handle this pretty easily, and a lot of the registrars actually have this in place. Yeah, yeah, Michele. Anyways, that is an important concept to actually get [to talk to if you get the time].

MICHELE NEYLON: Just bear in mind that Rod, at times, does not speak for the entire EWG when he makes certain statements.

ROD RASMUSSEN: I mean, it is a work in progress.

MICHELE NEYLON: It is a work in progress. I mean this is part, again, your feedback, your input on a lot of this stuff, it's helpful. I mean, we may have a lot of expertise, a lot of knowledge, but we need your input.

UNIDENTIFIED FEMALE: I need to jump in here and cut Michele off before we hear about the Irish postal system and how difficult it is to validate.

So I think we're going to trot through this fairly quickly, but we will be hanging around, so please hang around with us if you're interested in going on further, but I'll try and stick to my 15 minutes.

There is a section in here, and we passed around these documents on the privacy chunk as far as they would go. I think we only had about ten copies so they didn't quite, so please share.

And basically, as I said the other day, there's four kind of areas where we looked at privacy implications. There's obviously application of applicable law in the different jurisdictions. There is binding corporate rules, which is basically a privacy policy that we have made a commitment to. There is improvements in the privacy and proxy services, which we would prefer to call "shielding" and proxy services. And there is a secure protected credential for individuals and groups that are under threat.

And, of course, a key element in this whole accreditation system is the notion that people don't have an untrammeled right to get at your data, so that's a privacy protection in itself.

Okay. Are there people around the table who understand what we mean by "binding corporate rules," other than the ones that have heard me go on about them already? No? Okay. So I think it probably is worthwhile spending a bit of time.

It's not the most accessible concept in international data protection, but those who are familiar with the European framework for data protection know that there is a provision there that you're not supposed to export data outside the legal framework in the community to jurisdictions that do not have adequate data protection.

Global corporations – and I cite Hewlett-Packard just because it's one of the many that have operations in many jurisdictions – they've signed on

to binding corporate rules. So have people like Shell and Rabobank. Basically, what it does is come up with a set of management practices that meets a high level of data protection.

You select a data protection regime within the European community. You take your set of management practices or privacy policies and procedures to that data protection commissioner. They approve the policies and the procedures, and then that is accepted by the Article 29 Working Party for data protection within the Union. That means then you don't have to go to a data commissioner every time you export data. You're more or less accepted to be meeting that standard.

That, in my view, would be a dandy thing for ICANN – if it's interested in public policy obligations – to sign on to binding corporate rules. However, our remit is only the RDS, whatever you call it. So we can focus on the RDS and cover data transfers through the central repository to jurisdictions where there isn't data protection. Okay?

This partially answers that rather long question that came in a minute ago that someone said "duly noted" to. I mean, one of the problems of – and one of the reasons why I support a central model – is it's way easier to handle these kinds of issues if you have it in one place and you can set high standards and have management practices that you can have a hope of covering.

So anybody got any questions on the binding corporate rules? I have to say that they might not be accepted by a data commissioner within the Union because if you're trying to take only a piece of all of your

corporate practices, that might not pass muster. But in any case, it wouldn't hurt to have the practices. Steve?

STEVE METALITZ: Yes, I was just trying to understand who is the corporation that you would be referring to in this case? Is it ICANN, or is it the registry? And on whom would it be binding?

UNIDENTIFIED FEMALE: Well, it would have to be ICANN setting the policy, and that would be enforced through contract, which makes the binding corporate rules concept real lumpy. It doesn't really work well.

There's debate here, and you're not going to find out until you go to the Article 29 group and get an opinion. There's debate over whether ICANN is a data controller or whether it's not. Michele and I fight about this all the time. I think it's a data controller because it sets policy. It sets policy which it obliges people to do, observe through contract. RAA, you're setting policy when you said all those things in the contract.

So if you check on the Article 29 Web site, you will see a long document about what it means to be a controller and what it means. They did this in the context of the new review that's going on right now, and I'm pretty sure we fall within controller (we being ICANN).

So, I don't think ICANN can turn around and say, "You – all of you lot out there in the ecosystem – you all have to have binding corporate rules." I think that would be a bit of a reach.

STEVE METALITZ: But if I understand you correctly, you're saying that ICANN already has binding corporate rules, because it does set…

UNIDENTIFIED FEMALE: No. No.

STEVE METALITZ: Let me finish. It does set the policies that all of the registries and registrars have to follow. The piece that's missing is it hasn't gotten those policies blessed by the appropriate data protection commissioner in one continent that needs to approve them for them for them to be binding corporate rules under the European definition. Is that the main difference?

UNIDENTIFIED FEMALE: I guess the reason why I immediately said "no" was I think you're right insofar as we are enacting policy by creating requirements, but we have not stated the policy. And that's why I think it's high time ICANN stated the policy. When it gets into these intractable arguments with the Article 29 group, it's usually because they're saying, "What's your purpose?" and we haven't stated the purpose.

In the RAA agreement, the data retention requirement only works if you've already stated that you are going to collect, use, and retain information for the purposes of law enforcement, which hasn't been stated. So I'm begging for a statement of policy. Anyway.

STEVE METALITZ: And that was discussed in the WHOIS review team, which I see Susan raising her hand. But I think I understand what the distinction is now.

UNIDENTIFIED FEMALE: But we also did not agree as a team that ICANN was a data controller.

UNIDENTIFIED FEMALE: Oh, absolutely not.

UNIDENTIFIED FEMALE: That has not been agreed upon, and it may be the RDS that would have the binding corporate rules. That's up for discussion, yeah.

UNIDENTIFIED FEMALE: Wendy?

WENDY SELTZER: Yeah. I'm not deeply familiar with this idea, but I like it – what I've heard of it – as a way of putting some enforcement on the side of privacy. But there is a great imbalance here in the compliance that we've seen demanded of ICANN so far has been compliance coming down on registrars for data inaccuracies or for failures to complete enough of the WHOIS reveal information.

And we need corresponding pressures to protect the information that registrants are demanding – rightfully demanding – privacy for. So giving

them a means where the harmed individual isn't the only one who can demand redress but that there is some corporate compliance and audit function watching to make sure that that privacy is protected adequately I think is important for individual privacy and important for ICANN's compliance with international law.

UNIDENTIFIED FEMALE: Okay. Carlton?

CARLTON SAMUELS: Yeah, I just want to add one thing. It's very important to understand that you have to have something like that to scale. When you're moving from a 20-something gTLD to close to 2,000, you really need a different framework so that it scales.

And that is one of the reasons why this is so important. You're quite right. We're expanding the compliance arena, and you have to have some kind of framework that scales from this 20-something – which is very drafty, we know – to something that is a lot more useful for a 2,000 kind of gTLD in this space and taking on more issues to make it better.

UNIDENTIFIED FEMALE: Okay. Failing any other comments on that one, I'm proposing for the purposes of time because there's a very lengthy discussion of the privacy and proxy services in the actual document that was handed out.

I don't think it's new ground for people, because they've heard it before, and there is a PDP starting on the privacy/proxy services. We are

preferring to call them "shielded," to be a little more precise about what the service gives you and who's responsible for what.

But the important things are that if you're using a proxy service, it's the proxy data that goes in the RDS. If you're using a shield service, your real information would be in the RDS. It just wouldn't be released.

Have I got that right, folks? Yeah. Okay, good. Moving along to the next concept, which is the secure anonymous credentials.

JAY DALEY: Sorry.

UNIDENTIFIED FEMALE: We did talk…

JAY DALEY: Sorry. So you're not allowing any discussion about the privacy/shield services?

UNIDENTIFIED FEMALE: Oh, certainly. Go ahead, go ahead.

JAY DALEY: Okay, lovely. Right. So two things then. It's very common for corporates to use their lawyers to register a domain name with for the initial bit of a product launch or something like that.

What's your expectation there? That those lawyers need to register to become proxy service providers, or that they don't user lawyers, or that that carries on? Is there a way people can gain things there? Because I think it's extremely unlikely that every law firm can do this, and there are lots of small law firms that difficulty doing that.

UNIDENTIFIED MALE: Hopefully I'm not speaking out of turn, here, so let me know if either one of you. Yes. So the whole purpose to all this, right, is this baseline of accountability and contact-ability. And so when we've talked about this issue of a lawyer coming in or an agent coming in and registering for you, their information would all be there. They would be contactable, but the issue is that they would also be responsible.

JAY DALEY: Yeah.

UNIDENTIFIED MALE: And so, the reason that someone might go to – I'm assuming a lawyer would take responsibility for his client or reveal – but that wouldn't be the case for my friend who signs up for me. They probably wouldn't have the same interaction as an attorney-client privilege. So that's why someone would use a shield or an anonymous access instead. But it would clear that if you've put your name in there that you are responsible.

JAY DALEY: Okay, so it's understood that lawyers will continue to keep doing that. They won't need to become proxy service providers, and there's no chance of gaming or problems going on there.

UNIDENTIFIED MALE: I think that that's what we would agree on because there's enough safeguard there.

JAY DALEY: Right. Okay, great. Can I go onto the next bit?

UNIDENTIFIED FEMALE: Can I just put in the caveat that my problem with this is that it's really a question of fairness. Lawyers will invoke solicitor-client privilege and not reveal any details about their client. Others who can't afford that won't have that. Carry on.

JAY DALEY: Okay. Then what's the implication of that for this?

UNIDENTIFIED FEMALE: The implication is that if you want to be fully protected, you hire a lawyer.

JAY DALEY: Okay. Right. So the second is, have you got any plans about the separation of roles here between people who are going to be proxy

service providers and registrars and people who default as a registrar to also giving you the proxy service or anything?

Is there a potential there for people to start creating a registrar that is going to, say, be favored by particular types of users of domain names because of the way they operate proxy servers at the same time?

MICHELE NEYLON: If I understand the question, I think some of the stuff is going to be thrashed out in that PDP on proxy and privacy accreditation. The situation at the moment is that if you are a registrar and you have not signed the 2013 RAA and you run or provide a proxy or privacy service or whatever the hell you want to call those, you can do so however the hell you wish. There are no binding rules. There's no binding policy of any description whatsoever.

Once you sign onto the 2013 RAA, and the proxy/privacy service is run by a company affiliated with the ICANN accredited registrar, you have to follow some rules, which is it's kind of light. And then there's the PDP that's starting up now, which is having its first meeting tomorrow morning. I think it's at 8:30?

UNIDENTIFIED FEMALE: 8:00.

MICHELE NEYLON: 8:00? Oh, God, who schedules these things? Maybe come along to that, Jay.

JAY DALEY: Possibly. My question may not be for the PDP. It was specifically about the interaction between a registrar and a proxy service provider when they're under the same organizational control and if there is a risk analysis to see if there are any issues that could come from that.

UNIDENTIFIED FEMALE: That's an excellent point and we'll note that because when we do that risk and impact assessment, we might have a view on that. I have to figure that out. Thank you.

Just want to underline that one of the purposes of us putting this in the report is it comes under the accountability. We want more accountability. Obviously, the group is going to be looking at this, but in our view, this will give us accountability so that we can de-accredit the proxy service providers.

Okay. Now in terms of secure protected credentials, there is a rather large piece in the report here starting on page 41. And the concept here is that there are certain parties who need privacy for various reasons because if they operate a domain name and their address, phone number, personal data are revealed by an unsuspecting registrar, they could suffer harm.

The first example we give is religious minorities. The second example is called "domestic abuse" but it's really individuals whose countries have given them a change of identity, and many western countries do that,

for various purposes. People who would suffer harm if people found out where they were.

Political speech is obviously one of the more difficult ones if you're operating in the global situation that we're operating in. Ethnic or other social groups that are subject to harassment and journalists operating in war zones or hostile territory.

There are certainly other groups. Clearly, Doctors Without Borders are getting in trouble these days, so we would have to entertain that.

We decided that we should at least explore some of the basic pieces of this that need to be put together. The credentials are the easiest thing. The secure credentials that are on the market, and there is now kind of an "inspector" function or what you might call a "back door" that has been built in so that eventually you could if there were sufficient abuse of a use of secure credentials, they could be opened up.

But the point is that they would not be open-able within the ICANN ecosystem, so that it would remove the potential for the personal data to be revealed by an unsuspecting registrar when, for example, a dangerous spouse comes after suspecting that a domain's being operated by an ex-spouse. This puts it outside that system. It's a big overload, but it solves one end of the privacy problem.

So any questions on this? Everybody loves it. Nothing from law enforcement on this? No? Okay. Wonderful. Sold! Sold! We're out of time? Any last questions on privacy? Jolly good.

FABRICIO VAYRA: You good? All right, so take up the models. Alright. Do you want to scribe for me?

UNIDENTIFIED FEMALE: Yes.

MICHELE NEYLON: I'm just reiterating – I sound like a broken record – if you want to give us input, there's plenty of ways to do so. And we did try to address as much of the input we'd received today in the updates.

FABRICIO VAYRA: All right, so we're going to discuss the model. For those of you who were in the earlier session, sorry for the redundancy here in that. I'll just explain.

Obviously, in our initial report we put out a proposal for an aggregated system. That system would have followed generally this model: Registrant would give his information to registrar. Registrar would then take that information and give it to a registry. Registry would then, on a periodic basis – all registries – put that data up to an aggregated RDS.

And all queries for information of WHOIS, either anonymous or validated, verified, would just be between the user, requester, and the RDS. The RDS would not go back to registries for information.

After receiving a lot of comment, both I have to say in support and some questioning an aggregated model – so we had heavy on both sides – we

did a lot more thinking. And the thinking really was around how do we address some of the concerns around aggregating data while still maintaining some of the benefits of having aggregated data.

Obviously, when you aggregate the data, you can create unified policies around, say, privacy, protection, uniformity of display, validation, etc., and that's a very valuable thing that we didn't want to just walk away from because they're great concepts for the system.

What we talked about, it's detailed very heavily in the report, but just a high-level. Obviously, we've gone through many models, but the two that have kind of remained in our report are this aggregated that we initially came out with, and after analyzing six models including the aggregated again, we came out with a federated model.

Now the difference there is the data goes all the way from registrant to registrar to registry, just as we have today in thick WHOIS and which will inevitably be across the board for everybody. That data then isn't duplicated up to the aggregated or the RDS. What will happen is requestor will go to the RDS, make a request, and the RDS will actually go real-time and be able to pan across registries for data.

The main difference is, in some respects, think of it this way. It solves a lot of issues about jurisdictional concerns, where data sits. It solves a lot of issues around aggregating the data and housing it in one spot while still hopefully maintaining a lot of the benefits of having requestors only going to one place, being able to put in certain policies and principles in place without having to accumulate all the data in one spot.

We wanted to open that up for discussion and see if people still had concerns, thought of ideas or tweaks around these two concepts, kind of open the floor up. And if you have another idea, by all means, feel free to tell us. Just keep in mind whatever comments you make stand between me and beer, and that can be on the record. So, well, you're buying the first one!

JAY DALEY: Yep, no problem. I had enough of it last night. Can I just double-check that you are saying these as an either/or and not considering a joint model of the two of them?

FABRICIO VAYRA: So explain. How would you join the two?

JAY DALEY: Okay. So each of these has different characteristics that support different uses. If you're a law enforcement and you're worried about being tracked, then the aggregated data model's better for you because there'd be a single place that needs to be controlled, audited, and things like that.

If you're anyone other than law enforcement probably, then the other model – federated – is going to be better for those providing it because they'll feel they're under better control of it, and they're also less worried about who else is seeing the data about what's being accessed there. Okay?

FABRICIO VAYRA: Well, no. It's in the documents they just circulated, correct? The models? No, because the only really difference is, is that data copied into aggregate? Not that you don't have access to it or that people see different things.

JAY DALEY: No, no. Okay. If I am running one of these, then I would like to know who is looking at it. And I would like to be able to track them unless they were people who shouldn't be tracked like law enforcement.

And so it would potentially suit that we had both models whereas difference classes of usage used a different type of model so that law enforcement used the aggregated data one, which is operated under a certain set of priorities that ensure that there was no tracking taking place, and everybody else used the local federated one, which could be tracked and other things could be done with that.

FABRICIO VAYRA: So, you're basically saying, "Make a copy for that highly verified…"

JAY DALEY: I'm not actually saying that. I'm simply wondering if you're considering that as a possibility for a joint model across those.

FABRICIO VAYRA: We hadn't. We hadn't.

JAY DALEY: Right. Okay. Because, actually, there's a lot of implications about that that I haven't thought through, you know, surveillance being top of the list.

FABRICIO VAYRA: Yeah. And the reason I think probably we hadn't is because one of the things that led us to consider so heavily the federated model was the fact that we wanted to address some of the concerns around aggregation.

And so by having the two, we don't address the issues that people came up with us about, well, [inaudible] wouldn't be an issue because you'd have the two. But the aggregation and security risks and privacy, someone cracks the one system with everything in it. Stephanie.

STEPHANIE PERRIN: I actually think this just proves you don't listen to me, Fab. I think we did discuss this, and one of the problems from a privacy perspective and a trade perspective is you're basically setting two classes of requestor.

Understanding that law enforcement is different, but then you're throwing the civil law enforcement folks into different jurisdictions where they may get differential treatment, and that's going to become an issue over the years, I'm sure, as more economic activity takes place on the Internet.

It also doesn't solve the privacy problem because you will be exposing people to that type of inquiry in varying jurisdictions without protection.

FABRICIO VAYRA: We've noted your, I mean, we'll go back and look at it. Steve?

STEVE METALITZ: Yeah. Just one question about that. As I read these charts, under the federated model the RDS would still handle all the auditing. That would still be centralized. It would be centralized in a different place than the data was, but you would still centralize the administration of the gating system and issuing credentials and auditing.

So I'm just not sure what would be gained by this mixed system because the real question is what are the auditing rules for different users? Would you have different auditing rules for different users? But if they were administered in one place, it doesn't necessarily matter whether that's also the place where the data is stored. At least that's my understanding of the federated system.

FABRICIO VAYRA: That's why we did what we did. And I wanted to note, I mean obviously we noted it because it's an interesting concept that I think maybe is just worth, you know…

JAY DALEY: If I can come back then, sorry. This is the one bit of the report I haven't read well enough, then. I think that you ought to consider a slightly different model where the RDS is used as a lookup by the gTLD registry of the federated, of the person. So if someone comes to the registry to get the data, okay, and you then go back to the RDS to double-check about things.

Do you see what I mean? So rather than it be the gateway, which I think I understand now for the way the lookups are then spread out and things like that, it is used, you know, in reverse. Does that make sense?

FABRICIO VAYRA: Yeah. In some respects, to me, yes. But I think then you lose some of the other benefits of not having to find every registry when you do something, especially if you're doing a search. Say I'm looking up a bad guy who goes across multiple registries. I'd prefer to go to a one-stop shop who does the work for me as opposed to going to each registry and have that registry check my validation.

Is your concern the data's flowing up to the registry?

JAY DALEY: No. It's about the [inaudible] control. What you've described as a federated system is actually still a centralized system. Yeah, it is. You haven't actually got away from a centralized system here.

FABRICIO VAYRA: We have insofar as that we don't aggregate everything in one place and make a copy.

JAY DALEY: But, you know, metadata is actually as important as data, and this is centralized metadata here.

FABRICIO VAYRA: Correct, and we don't get away from process and transport.

JAY DALEY: Yeah, meta, yeah. But in many of the debates about surveillance that have taken place recently in the media, people have been saying, "Oh, no. We didn't actually look at any data. All we did was look at metadata." Okay? And people are just as upset about metadata being looked at as data being looked at. So you've actually got a hybrid model here of centralized metadata.

UNIDENTIFIED FEMALE: As best you can.

UNIDENTIFIED MALE: Yeah, I mean, it's…. Yeah, go. Lisa?

LISA PHIFER: So if I might, I think actually what your concern is, is that you want to have a different portal with a different set of policies around it and that's actually separate from where the data is stored?

It's an interesting thread to follow, but I think that's what your concern is, is that you want the access to for a certain set of highly-credentialed users to operate under different policies with regard to auditing and tracking.

JAY DALEY: Actually, no. This second one is a separate point, which is that the federated model that's being presented I don't think really is a federated model. It is a federated data model but a centralized metadata model. That, I suspect, once it's worked out people will have the same level of objection as the previous model did.

But the earlier point that I was making was, yes, that if you want to actually prevent tracking of law enforcement, then you might need a fully centralized data model at the same time. Sorry, I'm not helping you here. I understand I'm complicating things more.

FABRICIO VAYRA: No, no. Jay, so let me ask you something. I think I understand your concerns. So would the solution to your concern be that you go to one place to get your credentialing, and then you could actually just use that token or that credential across registries who then continue to just offer their port 43 or their, you know, just a regular WHOIS.

CARLTON SAMUELS: Yes, and that's what I thought I heard you say, that you want a central place for credentialing. But if you do that, you're still exposed to centralized metadata. You can't get away from that. You're not getting – as a matter of fact, that kind of metadata is even more important because it tells me who wants what.

UNIDENTIFIED FEMALE: Stops you from running a secure card.

BOBBY FLAME: Actually, I don't think it would because if I'm logged in under a centralized server that's determining what my credentials are, all it's doing is determining my credentials, right? And then it refers me somewhere else where we actually make the queries that I'm asking of the database. So, in reality, that would be a much more secure model in terms of my information. You're shaking your head.

CARLTON SAMUELS: Well, it's not even the security that was at issue here. It's whether or not you are keeping centralized metadata.

BOBBY FLAME: All you'll know is that I logged in. You won't know what question I asked, and what I don't want you to have is what question I asked, not that I logged in 12 times today.

UNIDENTIFIED FEMALE: Do we trust you to get the right [inaudible]?

BOBBY FLAME: That's what your credential means.

CARLTON SAMUELS: I'm not so sure because I have to know something to direct. What would you give me to direct you?

BOBBY FLAME: My credentials. I log in and I say…

CARLTON SAMUELS: And what do I do after that? If you come up to me and tap me on the shoulder and say, "I am me," and I say, "Okay, yeah, you are you, so bug off."

BOBBY FLAME: I'll tell you. I can answer this fairly simply, right? So, I log in. I say, "I'm Bobby Flame with the FBI and I'm doing…" and that's it, right? And you know that because I've logged in that I'm about to go ask questions that I don't want to be tracked.

You will either send me to some place that doesn't track and then I will ask my questions, or you will send me where you send everybody but it will include some check that says, "Don't track this guy," right?

So in either case, it doesn't matter to you what question I'm about to ask. All that matters to you is that I presented my high-level credentials, and you're going to give me high-level credential to untracked access.

CARLTON SAMUELS: Yeah, I get that. But sometimes, it's the question you don't ask me that tells me more than what you ask me. I mean, if I were surveilling somebody and the fact that you tell me that you don't want to be tracked, the fact that I know you say you don't want to be tracked is going to give me heightened, what-you-call-it, need to find you by other means.

I'm trying to make the case. I'm trying to figure out why it is it's important to have the metadata centralized in one instance but not for the other instance, which is the law enforcement requests.

BOBBY FLAME: I'm actually not – whatever the structure is on the back-end, I don't care. I really don't. You guys do it however it is you want to do it. You guys know a lot better than I do how to do this.

What I care about is that I can log in, and I don't care if you record the fact that I've logged in. What I care about is that you record what questions I'm asking. So as long as I can log in and then be sent and then be able to ask questions without my questions being tracked, I'm good. We're happy.

FABRICIO VAYRA: Can I ask a quick question?

BOBBY FLAME: Yeah.

FABRICIO VAYRA: If it came in and said, "Hi, I'm Bobby Flame. I've got this credential," and all he did, Bobby said, drop-down, "My purpose is investigations," and it stopped there and didn't track who you were investigating, does that solve your question?

BOBBY FLAME: Why do you want to track my purpose once I've logged in at that level?

FABRICIO VAYRA: Just asking, just asking.

BOBBY FLAME: I mean, that actually would probably be fine, but my assumption was that what you were going to do is you were going to credential law enforcement people as law enforcement people, and you were going to credential IP people as IP people. And the law enforcement people would be handled differently once they were inside the system than, say, the IP people would be handled.

So you don't need to ask me what it is I'm doing in the system. I log in as a credentialed law enforcement officer, you handle me one way; I log in

as a credentialed IP person, you handle me differently. And the only thing that really has to be handled differently is the tracking, at this point, and what data I get access to if you guys set different tiers for me.

UNIDENTIFIED FEMALE: Maybe we should start a queue?

FABRICIO VAYRA: Yeah. So start over here and then Lisa, Stephanie, and Jay.

JUSTIN MACY: Hi, my name is Justin Macy. I'm here for LegitScript. Something that we've noticed in all five of the models that are proposed is that it still has a centralized data requesting process. The data is in a lot of places, which is kind of what we've discussed repeatedly, but it still would have a centralized process for processing that.

We think one of the benefits of the Internet in general has been the decentralization of data and the redundancies in doing so. Is there a fear that having one organization having access to all of the world's WHOIS data like that is, in some ways, monopolistic or all intents and purposes? It's very valuable data.

UNIDENTIFIED MALE: That's good. Do you want to answer right now?

FABRICIO VAYRA: So, listen, I think that's part of the comments that we received both from either centralized portal access or centralizing the data generally. That's something that we're balancing out.

Obviously, the reason – hopefully, it's obvious – the reason that we continue to push towards some sort of centralization from a user policy and systems perspective, things become a lot easier. It becomes easier to manage rules.

It becomes easier for users to know that that's the one place. One of the things we hear a lot about is, "Where do I go to find this information?" People don't even know where to start. You make it a one-stop shop, they can do that.

And then you can start more easily tracking. Like, say, some of the concerns that Stephanie has brought up. If we start allowing every person with data to set their own rules or to do something different, let's put it this way, even if we said that everyone had to do the same rules, it's harder to police that.

So if we say, for example, "you need to credential yourself to get in as law enforcement to get access to special things," it's much easier to police that from a centralized space than it is from "well, everyone should do this." Because next thing you know, there's going to be a registrar or registry who isn't going to follow that rule, and the credentialing isn't going to mean anything and then sensitive data's going to get out.

So that's the perspective we've been looking at it from, and your concern doesn't go unnoticed. Yeah, go ahead.

JUSTIN MACY: On that note, obviously this data is used in many ways. There are many companies who use this data. Would this stifle innovations in this area?

FABRICIO VAYRA: We would hope not. I mean, look, one of the things that we've actually talked about – and we actually said this today – was that registries themselves if in the federated model would be able to open up their own access to either their clients or put up their own portals.

So this isn't to do away with people who, for good purposes, offer services around this. We're not trying to preclude that all. If we haven't accounted for it correctly, we will. Thank you. So we were going to go to Lisa.

LISA PHIFER: So I had one quick question or clarification, and then I believe Alice has some questions from the chat room also to interject.

The question was, you asked about sort of flipping the model on its head. So in that case, law enforcement would go through the registry, demonstrate they're law enforcement, ask the RDS to approve that yes, in fact, you are, but the registry would still see what you're asking, correct?

JAY DALEY: Yes. In that case it's law enforcement. I mean, I was talking about flipping the model more generally, not just for law enforcement, actually.

UNIDENTIFIED MALE: So I told Stephanie she could go next.

UNIDENTIFIED MALE: Yeah, I just want to go to this issue of how law enforcement is credentialed. It's one of the big sort of headaches. And, I mean, the easiest thing would be for countries or jurisdictions to have a central portal through which they authorize their law enforcement people, then they police it.

Obviously, there's audit trails within except if you had, for instance, some kind of an anonymous credential that would then be at least measured how often you're coming in anonymously. I mean, if you're INTERPOL, obviously you're coming in anonymously fairly regularly. If you're not, you're going to want to know why, right?

So I think we have to figure this out, so it wouldn't hurt to give it your best thought and make some propositions.

FABRICIO VAYRA: Yeah. Definitely on the verification validation, or the validation piece, we need a lot of feedback and especially from law enforcement. So Jay and then Lisa.

JAY DALEY: I think that you are conflating two separate things here. One of which is the user experience, and the other one is the policy under which this system works.

The word “redirection” was mentioned earlier, you know, as though the RDS is providing a redirection service to simplify the nature of the request there. Okay? I don’t think that’s something that you should be looking at within the system.

In fact to me, the whole way that the RDS is set up here is – as the gentleman over there said – interfering with the ordinary innovative process of the Internet, of the way people do these kind of things?

And you need to provide the underlying system there, and let other people find other ways of doing it and innovating and do these things. You can’t design a single global user experience like this. That just doesn’t work.

And I also think it’s unnecessary. I don’t understand what redirection the RDS would be doing that actually needs the RDS to be there. Is it saying, “Right, I want a specific data element,” and it therefore knows that only particular types of registry have that data element and it narrows that? In which case, publish it as a list, okay? We’ll build it into our systems and know which ones to go and look at of those registries.

There’s nothing there that it needs to do that couldn’t be done easier or better by people in their own systems, and it eliminates that single point of failure for the transfer of requests through and things.

FABRICIO VAYRA: I don't know who did use the word "redirect." I don't recall I did. But I will say, I guess one of our thoughts around centralizing aside from being able to set policies and stuff that would be much easier to police than just saying every registrar and every CCTLD and etc. just do what you want and then we'll just keep it on faith or do an audit on you.

Aside from all of that, I think it's clear from community feedback – that's why ICANN actually took upon itself to try to create a centralized WHOIS portal – because one of the major complaints we get from everyone who doesn't come to these meetings, including many people who are interested in use data…

JAY DALEY: Sorry, but you can easily create a centralized WHOIS portal without ensuring that the only thing that exists is a centralized WHOIS portal. Okay?

FABRICIO VAYRA: Well, that's in the federated model. It actually says you can create a centralized WHOIS portal, but every – this I do know I said a second ago – every registry and registrar can then decide on its own to provide that same data that they hold to every customer and/or everybody. So, in essence, what we're saying is exactly what you're saying.

JAY DALEY: Okay, you're going from two extremes of a spectrum there of a single global portal over there to complete have-to-build-it-all-yourself over here entirely.

FABRICIO VAYRA: No, no, no. It's a complete mix. What we're saying is that we will offer the one-stop shop with everything in it, and then if somebody wants to offer services on the side, they could build it.

JAY DALEY: But if somebody wants to build a separate global portal, the works, that way, fully accreditation…

FABRICIO VAYRA: Well, it wouldn't be global. But that's the difference, it wouldn't be global.

JAY DALEY: Exactly, that's it. That's what I'm saying. You're defining the one and only global portal that can exist, in this case. And I think that it's perfectly possible to do this in a way that allows multiple global portals.

FABRICIO VAYRA: Multiple global portals. Okay, no that's a very good point.

BOBBY FLAME: I don't want to, not to be a pain, but I don't want to have to be accredited through multiple portals in order to gain access.

JAY DALEY: Just one accreditation. Just one accreditation, but different levels of service and different ways it's offered.

FABRICIO VAYRA: Yeah, no, I totally…

JAY DALEY: Yeah?

FABRICIO VAYRA: Yeah, totally. Lisa, sorry.

LISA PHIFER: Kathy Kleiman has two questions. First question is: "Stephanie raises very important issues and questions about civil incrimination law enforcement jurisdiction, scope, and differences. The GNSO committee may not have this type of expertise when it evaluates this material. How does the Expert Working Group envision this very sticky material being handled by the community?"

FABRICIO VAYRA: I didn't hear you well, so I didn't know.

LISA PHIFER: Oh, do you want me to repeat?

FABRICIO VAYRA: I got that important issues, expertise that we may not have.

UNIDENTIFIED MALE: "Stephanie raises very important issues and questions about civil incrimination law enforcement jurisdiction, scope, and differences. The GNSO committee may not have this type of expertise when it evaluates this material. How does the Expert Working Group envision this very sticky material being handled by the community?"

FABRICIO VAYRA: Stephanie, do you want to answer that or do you want me to take it.

STEPHANIE PERRIN: Apart from the joke you're going to have to pay me to sign up for the next one of these, I think that that is a real issue. We're going to have to recruit people who have expertise in some of these issues to join that PDP, if that's what we're talking about. This is the GNSO community evaluating, though, that she's speaking of. So maybe that means intense reaction with the committee.

Even though I was teasing Fab about not listening, there's hardly a model we haven't at least trashed about for a bit. So maybe that means we're in for another six months. Who knows?

FABRICIO VAYRA: Lisa?

LISA PHIFER: Kathy's second question is for Bobby: "Is being law enforcement alone enough to open up unlimited use of the database? Are we concerned about what Syrian law enforcement or Chinese law enforcement might do with broad and unlimited access to WHOIS data?"

UNIDENTIFIED MALE: Yes.

BOBBY FLAME: Hi, Kathy. Well, that is a concern. You know, once you start tiering the access, and we have always, I mean, this is my personal advocation that it always becomes a difficult issue when you tier access for law enforcement only because we have a lot of operational security folks like Rod here, other people that do a lot of good works, a lot of good gumshoes, which is where we get a lot of our leads.

So that's why we wanted it to, you know, we've always advocated at this point for broader access for everyone not just specific tiered access for law enforcement because then you do run into problems as Kathy Kleiman mentioned.

It's like, "Okay, well, if you have law enforcement from certain countries which other people may not have faith in, you know, then you do run

into a problem" because if they have specialized access then that does become a problem if they're not using it for the purposes which we as the FBI would use them, which is for law enforcement investigations on crimes based in the United States.

So it does become a problem, and we've had these discussions before with giving law enforcement private access. If I wanted to be selfish, I would be like, "Yeah, I want the private access, and we can give everyone here at the table private access."

But what about the other law enforcement that aren't here? Or, like I said, the other advocacy groups who do operational security, who do work phishing like the anti-phishing working group, the messaging anti-abuse working group? People like that, who actually provide us with a lot of leads and a lot of intelligence and assistance.

So the whole issue becomes very sticky, and that's why have always as law enforcement advocated the most robust public system that is accurate and accessible to everyone. And we know it's difficult. We know it's a lot to ask, but to just be fair to everyone that's what we've always asked for. That would help us, and that would help the greater community as well.

FABRICIO VAYRA: Thank you, Bobby. Denise?

[DENISE MICHEL]: Yeah, I just had a follow-up question for Jay. Under the scenario you expressed where we would give the sort of list of rules on gated access

for purpose to the registries and then they would create the system or build it and implement it, wouldn't the registries be concerned about the cost that goes directly to them, to do that, the cost and resources versus keeping that in a more central location or a portal?

JAY DALEY: I wasn't actually thinking about the registries building that but alternate providers of this kind of service doing that.

FABRICIO VAYRA: So, Jay, to your point. As you were saying, would the solution be basically put out requirements, an RFP or just put out almost like when you do API's, you know? There's a certain standard and once you do that standard, you get feed into our tool.

Would you be saying, basically, have a validator or verifier who does everything and if you meet the certain standards or requirements, there could be multiple portals all of which may have certain nuance but at base floor all operate under the same rules and have to use the same verification codes and all have access down into the…?

JAY DALEY: Yes.

FABRICIO VAYRA: It can do the same things?

JAY DALEY: Yes. I think when you separate out the creation of credentials, it's once the credentials are done.

FABRICIO VAYRA: Yes.

JAY DALEY: Okay, yes. Then the rest of it, absolutely, yes. I think it's perfectly possible to do that because, ultimately, if you have a set of rules that says, "For this set of credentials, only this data can be extracted in this way," every registry is going to implement that and not trust that to anybody else to do. Even if the RDS is doing that itself, we're still not going to take the risk. Okay? Because it would be practice for us to move that risk outside of the organization in that way.

FABRICIO VAYRA: Okay. It's Steve and then Lisa.

STEVE METALITZ: One element here that would fit into this is the question of the cost model, which I know is something you're seeking more information on. But it's one thing to say there could be alternate providers if they all follow these same rules, and if one of the rules is they charge what is charged for WHOIS now which is nothing, that may have an impact on it.

FABRICIO VAYRA: Okay. Lisa and then Stephanie.

LISA PHIFER: I think what I hear you asking for is actually multiple RDS operators, and we'd been talking about this as the RDS. But it sounds like you're asking for multiple incarnations of the RDS running under consistent policy and a consistent or a common authentication and accreditation foundation?

JAY DALEY: Sort of, yes. I think you should recognize it as perfectly possible for the RDS to exist as a piece of desktop software. That somebody has something there on the desktop that knows the rules and goes and communicates with people and the system policies it because there has to be something that checks credentials.

The registries will have to ensure that credentials can only get access to certain sets of data. You're not talking about any aggregated limits across all registries that are a meta level there, so there's nothing that stops this being done in a piece of software on a desktop.

LISA PHIFER: Well, the one thing that might – and this is where I was going with my question – was I think you're actually only talking about it in the federated storage model, correct?

FABRICIO VAYRA: Yes, correct.

LISA PHIFER: Because you couldn't aggregate in multiple incarnations on everyone's desktop, right?

JAY DALEY: I'm trying to separate the data storage from the RDS component.

LISA PHIFER: Correct. Okay, thank you.

JAY DALEY: I'll send you a diagram to show what I mean.

FABRICIO VAYRA: Yeah, please do. We would love that. We would absolutely love it. So we're going to – I don't think there are any more people with their hands up.

FABRICIO VAYRA: Stephanie or Wendy?

UNIDENTIFIED MALE: But very short. Because of technical reasons, we have to stop very short.

FABRICIO VAYRA: Yeah. They're telling us to stop. So, sorry. Wendy and Stephanie? I think Stephanie was first. And then we're going to…

UNIDENTIFIED FEMALE: No, Wendy's first.

FABRICIO VAYRA: Oh, Wendy? Sorry. I apologize.

UNIDENTIFIED MALE: Microphone.

WENDY SELTZER: Ah, thank you for – sorry about that. Quick question since I didn't see in the skim whether you're considering sort of the possibility of delegation of credentials for access. And if so, so I have a credential but I don't want to perform the WHOIS access myself. I want to delegate it to someone else to do that on my behalf.

FABRICIO VAYRA: Now if anything, I think we've talked about it from a corporate standpoint, that a corporation might possibly have one credential that its employees use and the corporation would be on the hook for anything its employees do as an agent. But we've also talked the opposite of that, which is that that might go deeper than just a corporate level. So we're definitely, but not that I would get it, but I could hand it to somebody else.

WENDY SELTZER: And I appreciate that you're tying that consideration to the sort of contractual restrictions of "nobody could do more with it than I could."

FABRICIO VAYRA: Correct. Yeah. We want liability here. And then Stephanie?

STEPHANIE PERRIN: My question was actually a follow-up to Bobby Flame's comment on how law enforcement prefers sort of open access for all law enforcement. The only problem is that would be assuming all law enforcement was the same.

So there's a kind of fiduciary responsibility, not to mention a data protection responsibility, to ensure that a law enforcement agent from, let's imagine, Rogue State 39 is not going to come in and access trade information, access personal information, hand it over to criminal organizations, etc.

Which may be hypothetical. I would like to think it's hypothetical, but don't we have to protect on that? And that's the argument for certificates and for restricting access.

BOBBY FLAME: But to go back to Kathy's question, say you had someone from China? And they're like, "We have the procedure that law enforcement has

special access." How would you turn them down, or how would you turn down any type of nefarious police service?

The other thing is, people are using the WHOIS like they're going to get all this information. And this is my personal belief, we need to shut Google down, because that's where they're going to get the real information. I really don't think this constant obsession with WHOIS is…

JAY DALEY: Can we quote you on that? I got this tweet just lined up, Bobby.

UNIDENTIFIED MALE: This is recorded, by the way.

JAY DALEY: "FBI agent says they must shut down Google."

UNIDENTIFIED FEMALE: So speaking of shutting down, the technical people are now quite, quite over their limits, when they're supposed to be breaking down the mics. You are welcome to stay and talk. We are going to lose the mics now, though, because they need to go.

We really appreciate your participation. It's been a very enriching session, very informative. Thank you very much. And I think Fab wants to continue in the bar. He's buying everyone drinks so, please! Keep talking!

UNIDENTIFIED FEMALE: And also thank you very much for people on the line, because I think it's not so always easy to intervene when you're on the line. So thank you very much.

[END OF TRANSCRIPT