LONDON – EWG Final Report Discussion Session
Monday, June 23, 2014 – 17:00 to 19:00
ICANN – London, England

CHRIS DISSPAIN: Okay, guys, if you could take your seats, please, we'll start.

So everybody please take your seats. We're starting again.

Okay. One more call before we start. Please take your seats.

So thank you all very much for, A, being speedy and, B, being prepared to sit through the slide presentation.

Now, the purpose -- the purpose of this session really is for you to ask your questions. As Jean-Francois said, we would appreciate it if we could -- at this session, we could stick to questions on the report, on the presentation, and so on. I know that some of you may have some process questions. But as he's pointed out, we're still working with Stephanie on her dissent piece. So if we can roll those through to Wednesday morning, that would be fine.

I thought I would start just very briefly giving you the board's perspective just so that you know because Michele said, you know, "Stay calm, read the report."

I would say the same thing. Some of you would have been with the board and the GNSO yesterday when we talked about next steps. And really at this stage, the key is we're not in a rush. We're not suggesting that this report simply becomes implemented. We're not talking about

bypassing the GNSO. We're simply -- we've produced this expert's report and we acknowledge that it's long and complicated. And we want feedback on it.

So to be clear, there will be a series of Webinars, Q&As, et cetera, over the next period of time.

I know that -- I don't actually know what timing we're intending, but I would like to put a stake in the ground to say that actually we probably need to leave a reasonable period of time before we start those. People will need to come down from the joys of being in London. Those of you who live in the northern hemisphere and are European disappear for the whole of August for some bizarre reason.

So I think we need to be sure that we allow a little bit of time for the report to be absorbed. And certainly I think the board would appreciate that as well.

So we are going to have those. We have asked the GNSO to do some work for us. The main thing that I asked them to do yesterday was to give us a list of the things that they would like us to do before we give them a policy development process. To take a simple example, there are some things -- there are some things in the report that will require a deeper legal analysis than has currently been done and effectively will require legal advice. And I know that members of the GNSO would probably prefer that we did that first and so that they got the report with the required information rather than having to have them do it during a PDP.

So we've asked the council to consider the sorts of stuff they think we should do to assist with a report when it goes into the PDP.

We have never done this before. So we don't know really what the process will be. I want everybody to be really clear that the board wants to work with the GNSO community to come up with a process to run this through that is workable.

Now, let's have a discussion. So there's a microphone as usual. And I'm waiting for someone -- Steve, thank you -- to come to the microphone.

Steve, over to you.

STEVE METALITZ: Thank you. Steve Metalitz. First I want to thank the Expert Working Group. As someone who has been a 15-year veteran of the debates within ICANN about WHOIS, I think you guys have changed the terms of debate. You've delivered a game changer here. From now on, I think the discussion will be framed by some of these general issues, not to say where it's going to end up. But certainly the next phase here is going to be defined by what all of you have done. It's a very impressive piece of work. And, as I said, I think it's a game changer in a debate that had become very unproductive.

We're going to be looking at this. I should say I'm speaking here on behalf of the Coalition for Online Accountability which represents the copyright interests that depend upon access to this registrant data for many purposes, including enforcement of their intellectual property rights.

We're going to be looking at this very carefully and reading the bloody report, as Michele asked us to do.

And obviously there are a lot of tradeoffs here that we're going to have to kind of weigh pros and cons from our perspective. But I would like to ask about two other perspectives I think that are going to be very critical to the overall fate or reception of this proposal.

One of them is from the data protection authorities. One of the downsides of the current system is that many -- or some data protection authorities think it's illegal in some countries. I'd say over -- having observed this for 15 years, their bark is much worse than their bite on this issue. In fact, there has been no bite. That in itself is kind of a "dog that didn't bark" moment. It is very significant to me, but it is definitely an issue.

Therefore, one thing that I think will influence the overall outcome here is whether data protection authorities who had been complaining about the current system think that this system or something along these lines will satisfy their concerns. That's a huge issue from our perspective because if they do, that obviously is a big plus on the side of these tradeoffs.

The second one I would like to mention -- I don't know whether it came up in your deliberations. But in the first media coverage that I saw about this, the first one that actually kind of got it about what you guys were up to, the issue was raised about how this will affect the press and the media. And right now every day I see press stories that use WHOIS data. Any time anything weird or funny or sinister happens on the net, very often there's -- one of the factoids is who has registered the

domain name that is associated with that behavior that has been newsworthy for some reason.

I think it's clear from the slide about what's available to the public that journalists will no longer get that information, to be able to see those stories, unless they fall into one of the other purposes. So it is obviously a freedom of expression, freedom of the press issue here. And I would just ask whether that came up in your deliberations and how you think that ought to be vetted in order to find out what journalists, the media think about this aspect of the report. Thank you.

CHRIS DISSPAIN: Thank you. Steve.

Who wants to? Michele?

MICHELE NEYLON: I do enjoy going head to head with Steve, so I thought I'd try this one. Michele Neylon for the record.

On the data privacy thing, I'm very, very conscious of the issues around the current WHOIS. Most of you know that I've been embroiled in quite lively debate with ICANN on this matter.

Article 29 and others have written to ICANN on several different occasions expressing general discontentment with the current status.

Now, whether or not what we're proposing will make them very, very, very happy or not, I honestly don't know because I'm not them. But what we have come up with, I would think, goes a very, very long way

because we're moving the concept of making all the data available to everybody all the time, which was the main issue that they had.

If you look at the way, for example, the .EU WHOIS operates, if you do a Port 43 WHOIS lookup, you just get back the domain name available, unavailable, the name servers and the registrar. If you want to get more data, you need to go to a Web-based system which may be protected by some form of CAPTCHA.

And if you are a private individual, the amount of data is completely minimized. That has to be done in concordance with EU law because the .EU registry operates under contract to the E.U. Commission. So I would say what we are proposing should appease them. I'm not the expert.

I would defer to Stephanie, obviously.

CHRIS DISSPAIN: Did you want to say something? No?

I think your question about the media is very -- is a very interesting one as well. I mean, is there any way we could create an authorized state or purpose, if we wanted to? The question is: What would the purpose be, you know? To make fun of something because they have got an interesting Web site or something. But I take your point. It is a very valid point.

Carlton, go ahead.

CARLTON SAMUELS: Thank you, Chris. I was just running to the media question. We do recognize research purposes, and the media might be able to access in researching a story or so in that way. As long as the purpose is permissible, then they can get it.

Recall, we said we do not believe we covered every single purpose. So there could be other purposes established and as long as they're established, they're permissible. Thanks.

STEVE METALITZ: DNS research as was described here, it wouldn't cover daily press.

CHRIS DISSPAIN: That's a fair point. Absolutely.

Sir?

ALEX DEACON: Hi. My name is Alex Deacon with the MPAA. And I would like to also thank you very much for your work. It is an amazing report and appreciate very much the hard work that everyone put in. I have a more softball question to kick things off. I have many technical questions. We can put those off till later on.

But on the slide before this, the question was asked -- the fundamental question is: Does this meet the needs and, if not, can the current WHOIS system continue to meet whatever needs? I forget how it was phrased exactly.

So who's going to answer those questions or how will that question be answered? Because it seems to be that until we answer that question, we really can't move too far forward.

CHRIS DISSPAIN: It is a matter for the ICANN community, but if anybody else wants to say something else.

ALEX DEACON: It is us as multistakeholders. It is not the board. It is not the GNSO.

CHRIS DISSPAIN: No. It is the community.

ALEX DEACON: It is us.

CHRIS DISSPAIN: If this proceeds, it will be your fault.

[Laughter]

Jimson?

JIMSON OLUFUYE: Thank you. Jim son Olufuye. I would like to really congratulate the Expert Working Group for the great job you've been doing. I have had the privilege to be following or to have followed the outputs you generated over time.

Well, I just want to ask this question concerning audit. Audit provides assurance for the system. So I want to find out what measure of audit do you have imbued into the system or is it external? Thank you.

CHRIS DISSPAIN: Audits? Who is in charge of audits?

SCOTT HOLLENBECK: I think that was actually my subgroup that looked at this.

Jimson, if you look into the document, you will find a whole section of principles on audit and escrow.

We think it is an absolute requirement that there be records kept of the transactions that are being performed and who is asking, for example, so that people will have a right to find out who is asking about their data. So much more detail in the report.

CHRIS DISSPAIN: James?

JAMES BLADEL: Hi. Thanks. James Bladel speaking, just on my own behalf.

A question going two speakers ago, I think, you know, a question regarding next steps and the path forward from here. I think that there's some discussion within the council -- at least informally at this point -- on what the next steps are. It seems like there's some work --

there's a body of work that needs to be done to take from the output of this work to the input of a PDP.

My question to the EWG is: What would you like to see as part of a recipe for next steps and where would that occur? And I would submit that that starts with the GNSO Council.

CHRIS DISSPAIN: Were you here when I started? Because I talked about the legal stuff which you brought up in the GNSO yesterday.

JAMES BLADEL: No. I think Avri brought up something.

CHRIS DISSPAIN: No. Getting legal advice before we started.

JAMES BLADEL: I came in late.

CHRIS DISSPAIN: Okay.

JAMES BLADEL: So I guess what I'm asking the panel is --

CHRIS DISSPAIN: Sure.

JAMES BLADEL: -- I mean, what sort of things would they see as critical milestones that have to be hit between here and there.

And then a second question -- and I do mean this, you know, in a spirit of collaboration and not to be like up here throwing stones but, you know, we have this group now, we have concluded your work after an extensive period of time with these recommendations. I know Susan, Kathy, others, we were on the AoC authorized or mandated WHOIS review team as well.

How do you see your work interleaving with the work that came out of the WHOIS review team?

We heard that reference by Steve Crocker this morning that that work would continue, the implementation of those recommendations.

Do you see any friction there?

CHRIS DISSPAIN: I mean, I'm happy for anyone to answer it. I've got something to say, but you've got something Susan? Go ahead.

SUSAN KAWAGUCHI: So on your second question about, you know, how --

I think our experience and our report on the -- from the WHOIS review team definitely sparked this team to be created, and informed a lot of our decisions, and, you know, we used it as guidance: Where were the

sticking points that we had trouble with. Where did we have to stop because our mandate was this. We can't --

We, you know, had a -- we agreed upon, as a team, certain parameters to discuss, and we didn't have that here so we could discuss everything.

And so I think at least for me personally, the experience of the WHOIS review team really helped me participate in this team and maybe move the ball forward in our thinking on certain issues.

JAMES BLADEL: So while I don't want to diminish the value of that, I do, I think, have a more -- just a fundamental question of the recommendations that came out of the WHOIS review team.

Are there any of them that are now -- have been obsoleted by your work?

CHRIS DISSPAIN: No.

JAMES BLADEL: Are there some that support your work specifically? I guess I'm looking for what --

SUSAN KAWAGUCHI: More detail.

JAMES BLADEL: Not necessarily a scorecard, but I'm looking for a --

CHRIS DISSPAIN: James, let Margie or Denise respond, whatever would be easiest.

JAMES BLADEL: Sure. And I'll go ahead and sit down.

CHRIS DISSPAIN: That's fine. I'm going to respond to another part of your question in a minute.

MARGIE MILAM: This is Margie Milam with ICANN staff.

We've looked at this from a parallel approach, so we continue on the improvements on WHOIS until something happens on this side, and this may be a many-year process.

And so currently we're working on some of the implementations. We had a session on it yesterday with the GAC and I'm happy to provide a link to that. I'll provide a link in the chat. But yes, we're not doing anything at this juncture to set aside the improvements to the current WHOIS system.

CHRIS DISSPAIN: Yeah. Let me -- let me sort of take us back to the beginning of this.

So we -- the board approved -- the board approved the WHOIS recs and they are proceeding down the track that they proceed down. And you may not think they're being done fast enough or at all or whatever but they are on their track.

What then happened was that we got a report from the secure -- ICANN Security and Stability Advisory Committee which talked about -- in very, very blunt terms, about the need to go back to the bottom line, to Stage 1, and start again.

And that's what this working group was tasked with doing.

So the two things are entirely separate. This is a clean slate approach, which obviously needs to go through a whole series of iterations within the GNSO before anything else occurs, and then even when that happens, there is going to have to be an implement stage, and that may well take some time, et cetera, et cetera, et cetera, and it is certainly not the intention that in the meantime, WHOIS is not continued to be improved or whatever needs to happen. That's the first point.

The second point is that one of the reasons why the board decided that having this independent expert working group was a good way to start was because everybody acknowledged, including all of the GNSO, that if we started a policy development process in the GNSO on WHOIS, it wasn't going to work.

So the idea was to have this clean slate start to provide the GNSO with a series of boundaries within which to prepare -- to create its policy development.

So the goal has always been to provide -- I don't want to use the term "gates" because it has a different meaning -- boundaries in which you guys will work.

Now, the reality is we have never done this before, so now is the time for -- once you've all established, read the report, et cetera, et cetera, we need to work together to figure out what the next steps are.

Because you might say, "Well, do some stuff first." You might say, you know, "Let's use this methodology," or whatever. So that's the -- that's the -- I don't know where you've disappeared to, James, but that's basically the goal.

Sir.

PAUL KEATING: Hi. My name is Paul Keating. I'm a lawyer in this space. I represent a lot of third-party service providers who depend on WHOIS data and related data concerning domain names to serve up this data in a packaged manner, upon request from customers.

So I see this as -- I'm trying to figure out where these customers would fit in. They are commercial providers. Examples would be DomainTools who provides a huge swath of historical information relating to this -- this space we call the Internet. It's perhaps the only party who maintains historical data regarding registrations as far back as the -- as the mid-1990s.

So I'm trying to find out how my clients fit into this proposal.

It seems as though this proposal was driven largely from two points of reference. One is data protection and the other one is an attempt to centralize the WHOIS which currently is a very decentralized system with centralization being provided by third-party for-profit entities and some nonprofit entities who have, over the past 20-odd years, developed their business models surrounding the current situation, the current state of affairs.

So my first question, in terms of data privacy is: Is that not best addressed at the point of input? So allowing the user, the registrant whose interests you are purporting to protect, to determine the privacy that they wish to achieve with their particular information?

If you register the information and don't opt out, or you opt into the public sector, then your record is opted in, the same as if I bought a house in London under my own name, and it would be forever there. I could not go back and decide on Tuesday that I didn't want my records from 10 years ago to exist in relation to this residence.

The second thing is: I don't see a space in your authorization mechanism to fit third-party commercial entities. I just don't see one. We're not a research for the public benefit. We're a commercial enterprise such as DomainTools. Any other -- the registrar data, there are a considerable number of registrars out there who do not power their own WHOIS who rely upon third-party commercial services to, in fact, power their WHOIS systems.

So I would like to see the panel address that particular issue, so as not to carve out and not to unilaterally destroy or as a community destroy a

member of this community, a significant member of this community who's been active and participating for the last 30 years. Thank you.

CHRIS DISSPAIN: Fab, do you want to take it? And then anybody else on the panel who wants --

FABRICIO VAYRA: Hey, Paul. Thank you for asking that.

So it's actually something we discussed for probably at least a year -- or a couple months into the year and a half. I know that the earlier drafts that we put out said that the system should accommodate for ancillary services. I think that developed into specifically identifying reverse WHOIS and WHOWAS services and so I think you need to look at it from a perspective of we didn't hopefully carve that out. We just didn't explicitly tie the bridge between what Susan said, which is that we tried to encapsulate the universe of permissible purposes but we didn't -- we may have not captured all of them. I doubt we did, as you're probably pointing out right now, and as Steve pointed out on the news services on free speech.

So if you marry with the fact that you could add a permissible purpose through the community dialogue and marry that to the explicit statement that the system is and should be built to accommodate reverse WHOIS and WHOWAS, I think that solves what you're talking about.

And so really it's just an issue of in the report we just didn't explicitly tie "The system should be built in this way" and that specific purpose.

So I would just say it's something that I'm glad you're bringing up now it clearly identifies a place where it just needs further work.

PAUL KEATING: Well, I appreciate that but the groups that -- for example, brand protection, security, customers of DomainTools, for example --

FABRICIO VAYRA: Yeah. I'm one of them.

PAUL KEATING: Well, they don't use DomainTools for the linear purpose that you're describing.

FABRICIO VAYRA: Well, I'm --

CHRIS DISSPAIN: Hold on. Hold on. So two things.

This is -- so first of all, we're going to get down into the weeds on this, but Rod wants to respond to so let Rod respond.

ROD RASMUSSEN: Yeah. Actually, Principle 50 actually addresses this directly. We actually did put this into the document.

I'm sorry to correct you, Fab, but it's a big document and there's been a lot of discussions and we're actually looking at this as an opportunity to have, within the framework, an ability for third-party services like DomainTools and MarkMonitor and others that have provided these services over the years in some legal gray area to be able to at least interact with the system going forward.

It's important to realize that you have to have permissible purposes in order to gather and display that information, and as long as the system -- the third parties or whoever is involved are able to work and interact within that framework, they should be able to do that. And that's the way that we've tried to -- to design this document, to allow for that without precluding those kinds of services, but at the same time recognizing that you still have to provide the same kind of protections, et cetera, through some sort of third-party service as you would directly with the RDS itself. Right?

PAUL KEATING: Granted.

But if your goal of protection -- as you're using the word, if the goal of protection is to protect the privacy rights of the registrant, why not give that and empower the registrant to make that determination instead of trying to make it for them.

CHRIS DISSPAIN: Because that's --

ROD RASMUSSEN: We did do that.

CHRIS DISSPAIN: I mean, it's -- I mean, we have done it, effectively, but not in the way that -- not in the way that you've said.

But I think you've -- sir.

CHRIS PARSONS: Hi. Chris Parsons. I'm a post-doctoral fellow with the Citizen Lab with the University of Toronto.

I have three classes of questions and I don't know how long they are but they're significant.

The first addresses -- there's an alarm going off. Sorry.

The first relates to individual protection. I think that the idea that you have a protected gating system for individuals who identify at risk is very positive. However, it's only positive when you know or believe or suspect that you will be a person at risk.

It is incredibly often that journalists are no longer with a Reuters badge, a New York Times badge, or something like that. They're a blogger, they've registered a Web site, they've traveled somewhere in the world, and then they realized, when they landed, when they're seized, when they're detained, "I am a person of interest."

Humans, on an individual basis, do not have the capability to ascertain if what they say needs to be protected based on where they travel. In some cases they can; in others they can't.

So my question, my first, is: How do you account for that threat model? How do you account --

CHRIS DISSPAIN: Why do you need a domain name?

CHRIS PARSONS: That's not the point.

CHRIS DISSPAIN: It is the point, because --

CHRIS PARSONS: No, it isn't.

CHRIS DISSPAIN: It is a point -- it is a point --

>> (off microphone.)

CHRIS DISSPAIN: Well, he asked -- I thought he -- I thought he finished his question. Had you finished your question?

CHRIS PARSONS: That's not the point.

CHRIS DISSPAIN: Well, so we're now having a dialogue, which I thought was what this was supposed to be about, Milton, but thank you.

Do you have to register a domain name, though, to do what you're saying is what I'm asking you.

CHRIS PARSONS: I'm saying you don't know. If I'm a university student at the University of Toronto and I write about the kind of Myanmar in an appropriate way, should -- should I have known about that 10 years before I flew to Myanmar? I don't think that you --

CHRIS DISSPAIN: So, sorry, I misunderstood what you were saying.

CHRIS PARSONS: Insulting the king in that case can lead to charges.

CHRIS DISSPAIN: Yes.

CHRIS PARSONS: So I'm saying that people can become at risk --

CHRIS DISSPAIN: That's true.

CHRIS PARSONS: -- and the ability to query through a law enforcement purpose to identify who that individual is --

CHRIS DISSPAIN: Yes.

CHRIS PARSONS: -- they will not have known ahead of time that they were -- they were needing the protected credentials.

CHRIS DISSPAIN: So what would the solution be?

CHRIS PARSONS: I'm suggest -- I'm raising the question: Have you considered this as your threat model in identifying what a protected person is and then how would you preemptively do that.

CHRIS DISSPAIN: You need the microphone, Carlton.

CARLTON SAMUELS: Yes. We can't anticipate it for you inasmuch as you can't anticipate, but what we do is provide the possibility of being protected. So that is the reason for the secure protected credentials.

If you anticipate something is going to be happening to you, you avail yourself of that.

If you don't and it -- and at some point you change your mind, you come back to it and you, as -- we say in Jamaica, you wheel around and come again. There's no other way to do it. You, either anticipate it, and if you anticipate there is a way to do it, and if you didn't anticipate it, and at some point down the road you figure you might need it, then you -- you come around again. That's the only other way.

CHRIS PARSONS: Why not have that as the default, then?

CARLTON SAMUELS: I'm sorry?

CHRIS PARSONS: Why not have it as the default?

CARLTON SAMUELS: Because there are probably another hundred million reasons why that would not be the standard normal way to use a data -- Web site or domain name.

CHRIS PARSONS: Okay. That's fine.

The next was: So something that we heard in this panel, which I appreciated, was accountability, logging, an effort to identify who is

accessing records, and an ability for individuals to ascertain if their records were being queried, and I think that's a very positive step and it's very important.

However, it stands at variance from what was discussed in the LEA session earlier.

In that session, there was a discussion where ICANN -- or sorry, not ICANN, my apologies -- INTERPOL would act as a proxy service. There would be no way for an individual at some point in the future to know who had been querying their data. Various jurisdictions have right of request. There are expectations that individuals will have an ability to challenge requests for the personal data. And I was wondering how this system accommodated that.

CHRIS DISSPAIN: Well, given that none of us were in the -- were you in the --

ROD RASMUSSEN: I was the one that gave the LEA presentation this morning, so as I said at the time, the data would be -- the queries would be logged by the RDS system, whoever the operator is, what have you. Their queries could be proxied through an INTERPOL or somebody like that, who is also responsible for knowing who is using that data amongst which law enforcement agencies, et cetera, so that if the -- if there's abuse detected at the RDS level, it could be pushed down through the responsible -- and this whole idea around accreditating the accreditators would be able to then at that point be able to deal with an

abuse issue directly with whatever the law enforcement agency that was doing whatever they weren't supposed to be doing.

So there's -- the idea is that there's a way for people to proxy queries there, but they're still accountable for the activities that are going on within their accreditation sphere.

CHRIS PARSONS: At some point, would there be some notification to the end user the data had been accessed?

ROD RASMUSSEN: I'm sorry, I didn't --

CHRIS PARSONS: At some point, would there be a method within the framework you're developing for the individual to be notified or --

ROD RASMUSSEN: The individual to be --

CHRIS PARSONS: That their data had been accessed?

ROD RASMUSSEN: There data had been accessed at all, yes.

>> (off microphone.)

ROD RASMUSSEN: Yes. Now, because of the sensitivities around, in particular, law enforcement, they may not know exactly who and exactly when. That's all a matter of policy decision. But that -- that information has to be tracked and over time that information would have to be released in some sort of process. And the question is: Timeliness, level of granularity, et cetera, and that's all -- this is -- we produced a framework for -- in which to do that. There's a lot of dicey policy questions that are going to have to get down to the nitty-gritty on how that might work, but I think that the thing you're looking for is possible within the framework we're talking about. It just has to be dug into.

>> (off microphone.)

CHRIS DISSPAIN: I think it is important to understand that we have to try to maintain a fine balance between how much detail to go into. So we've tried to talk at a principle level on the basis that there is a policy development process that needs to take place to actually build policies around it. I think it is important that we are talking at a principle level and the granularity is a real challenge. And the real balance with this is to how granularity. If we did too much, we would be accused of mandating policy which is not what we are not trying to do.

Stephanie wanted to make a comment and then I will come back to you.

CHRISTOPHER PARSONS: I have just one more, yeah.

STEPHANIE PERRIN: I just wanted to respond to that. I made a rather flippant comment that the rules engine would be quite a challenge to build. Let me just respond in terms of Canada, which you know quite well, Chris. There is a big section in our data protection legislation about when the individual has a right of access, Section 9. The civil liberties group is planning to take it to the Supreme Court. Whatever happens with that, it would impact what was in the rules engine in terms of the timeliness, exactly what your rights are in terms of knowing what law enforcement --

CHRIS DISSPAIN: For the person in Canada?

STEPHANIE PERRIN: Sorry?

CHRIS DISSPAIN: For the person in Canada.

STEPHANIE PERRIN: For the person in Canada or the registry in Canada.

CHRIS DISSPAIN: Exactly.

One more, sir.

CHRISTOPHER PARSONS: You may have a very quick snap result. This is to Stephanie.

I'm just interested in her insight.

Again, in Canada, we recently had a Supreme Court decision that recognized a basic right to anonymity and established very high thresholds in order to get access to data which would arguably include that in a WHOIS system, which would include a warrant from a judge.

So in light of the Supreme Court ruling, would the rules engine then require someone from INTERPOL, or whatever the proxy happens to be, would INTERPOL then be responsible for evaluating the legal standards of the country who is asking for the data to make sure that the law enforcement officer --

CHRIS DISSPAIN: I know you want to respond. Let me just respond as a lawyer. You have to be a little bit careful by -- I think the answer to your question from a legal point of view would be yes, provided that it's actually legislation. There are decisions made, overturned all the time. That becomes complicated. If it is defined under the legal system in the territory, whatever it may be, if it is a common law system, et cetera, right, it may well be so.

Stephanie, you want to...

STEPHANIE PERRIN: Well, Chris, as you know, our government responded to the Supreme Court decision by not amending the legislation that is currently on the table. The legislation that the Supreme Court was responding to was, of course, the charter. So it's law. So we would have to build that in. Just as in the United States, we would have to build in whatever was there.

That's the kind of thing that is already agonized over in the Budapest convention with the instruments flowing out of that.

CHRISTOPHER PARSONS: Thank you.

CHRIS DISSPAIN: Hello.

ROBIN GROSS: Hi. My name is Robin Gross. And I'm interested in hearing about the dissenting opinion to the report that hasn't been published yet. I was encouraged to hear earlier this afternoon that that dissenting opinion will be published forthcoming. So I look forward to seeing that.

Stephanie, as the author of that dissenting report, perhaps you could tell us what led you to draft and publish that, what your concerns were. Thanks.

CHRIS DISSPAIN: So I've got, Stephanie, no problem in you replying. I would just remind everybody that you're still working on it. We're still talking about it. So we -- there is another session on Wednesday morning.

But you go ahead.

STEPHANIE PERRIN: Basically, there are a number of things that I had problems with. The precipitating factor was the content clause -- and I can't remember the number just off the top of my head. Basically, there is a requirement in there that individuals be given an opportunity to consent to the use of their contact data -- this is in the restricted area -- for all permissible purposes.

And in my view, number one, you can't pull out one provision of data protection law and make it sort of a cameo without the others. So consent has to be freely given. It has to be -- you know, you have to have an option to consent or not. It is clear that you don't have an option because of certain other principles that reinforce that, saying you either consent or you back out of the registration. Well, you know, that's a bit of an issue from a consent perspective.

So that caused me to also worry about a number of things about the gated data. And so there's a few issues surrounding the gated data. The fact that you are consenting to all permissible purposes -- we've heard a lot about the different purposes and how you are accredited for this purpose, not that purpose, you know, how transmutable your accreditation is, that all has a bearing in data protection implementation. So there's a lot of questions there.

And that's a reflection of just some of the details that aren't all worked out yet. It is not a reflection of the report itself, okay?

And then the third thing -- and you've heard quite a bit about how things are inside the gate or outside the gate. And in this presentation, we've got a big focus on it in the slides. The language in the report in my view is still confusing. And if I'm confused, with all due modesty -- and I have been saying this for several weeks now and people are probably ready to argue with me -- I'm not stupid. If I don't understand it, there's a good chance that somebody else isn't going to understand it. That's my -- that's my story, and I'm sticking to that.

I'd like to see that language changed so that it was more clear so you wouldn't get the idea that public actually is published within the gate. That's a little confusing.

CHRIS DISSPAIN: And I think it would be fair, Stephanie, to say, wouldn't it, that in our discussions we have established that there is -- at least I think we have, I hope we have, that there is a difference between the dissent -- the dissent piece is not "I think the text is unclear." That is something we would handle with editorial tweaking, and it is not necessary to publish -- in other words, we would as a result of some comments that you might make some editorial changes to the report. And that deals with the last point.

And I think it's also -- so we're talking about that. And I think it is also fair to say, Stephanie, there has not been an issue with any of us with

you having the right to dissent. And especially in respect to the conflict piece -- sorry, the consent piece which we understand your view on.

So let's -- Jean-Francois, did you want it say something?

JEAN-FRANCOIS BARIL: Just a simple thing. We discussed the three issues that Stephanie just explained yesterday within EWG. And I think we are very, very close to make it -- correct the way it is put in context, so the wording has been discussed. There's -- we are fully, in fact, not excited -- that's probably too much. But we are very, very happy that if there's some divergent view, we are very explicitly authorizing and promoting this divergent view because we cannot say this is accommodating everything. So this is one thing.

And I believe with what we discussed yesterday very soon, hopefully the sooner the better, we are going to be to post something. Stephanie would be able to put in the blog the response for this one and the dissent. So I think this issue would be solved.

Yes, this has been very much precipitated. I think it was maybe a question of time. Hard work from everyone. So everyone is very nervous.

And I missed the mark here. And if someone is responsible for this one, this is myself because I thought this was not giving justice to everyone within EWG to have the full understanding of the context of this dissent. That's what has happened.

STEPHANIE PERRIN: Very briefly. I'm afraid this whole dissent thing has unleashed a monster because it was suggested to me early on that I could dissent on -- put my thing up on my own blog. And I don't have a blog, and I always used to say people who blogged must be -- you know, don't have a life.

So I was talking to Mikey O'Connor about this. And he said, You ought to have your own name. You don't even have your own name registered. Not being a domainer, I didn't really care about it.

Anyway, I now have my own domain, stephanieperrin.com. And I realized as Mikey was walking me through how to blog, I'm going to love this. I have got five other topics I want to blog on. Don't worry like that, Chris. It is not all ICANN.

CHRIS DISSPAIN: We have created a monster.

STEPHANIE PERRIN: Indeed you have. It is fun and it is not hard. I'm going to put my thoughts up there.

CHRIS DISSPAIN: I think, Stephanie, just to be clear, the working group is fine with whatever you do with your blog. What we want to do is to get a piece we can actually put in the report and that's not necessarily the same as it would look like on your blog. That's really the key.

Okay. Let's move on.

ROBIN GROSS: Okay. I just had one other question, and this one is to the whole panel. How will you determine whether the purpose that an accredited actor puts down is actually correct?

CHRIS DISSPAIN: Do you mean for them to be -- you mean for them to be validated to have access?

ROBIN GROSS: To have access, yes.

LANRE AJAYI: That's simply through accreditation. During accreditation, the requester has to indicate his purpose and that purpose has to be validated before given credentials.

CHRIS DISSPAIN: Robin, did that answer your question? It did? Okay, cool.

KATHRYN KLEIMAN: Can I follow up to Robin's question?

CHRIS DISSPAIN: Aren't you next in the queue anyway?

KATHRYN KLEIMAN: I am.

I intend to be in line again and again, so I appreciate the two-hour block. First of all --

CHRIS DISSPAIN: Let me just say, if we are only here in this room because of you, you may find that everybody else is gone.

Go ahead.

KATHRYN KLEIMAN: First, I think you should all be wearing T-shirts that say "I survived the EWG."

CHRIS DISSPAIN: Absolutely.

KATHRYN KLEIMAN: As a member of the WHOIS review team, these are long, long processes. And thank you for your time, effort, creativity.

And so just in follow-up to Robin's question, let me ask: So you accredit the Chinese law enforcement or INTERPOL accredits the Chinese law enforcement which is a member of INTERPOL. And then China comes on to that massive centralized database and wants to look for everyone running certain types of pro-democracy Web sites critical of China and they're looking in jurisdictions outside of China particularly jurisdictions

with free speech, freedom of expression protections. How do you stop that?

CHRIS DISSPAIN: Rod?

ROD RASMUSSEN: So the good news on that is INTERPOL already has a protocol for exactly this because this happens in the real world or the existing world of law enforcement as it is today where the Chinese, or whoever, pick your favorite country, asks about people in another country that they have interests in.

Now, the INTERPOL has a job of coordinating those communications and evaluating how their current systems are being used in order to learn about suspects or persons of interest in other countries today.

They, for example, will be very helpful in solving international sex-trade types of things or pedophiles or the like. But they are not supportive of, typically, people going and doing those kinds of witch hunts you're talking about. And they have protocols for that.

And, frankly, whoever is making such requests is at risk of losing their access to the entire INTERPOL system by making such requests, right? They have a tracking system for taking a look at the kinds of requests that are coming through.

Will everything be perfect on everything and every request? No. We know that, right? There are human beings involved, et cetera. There is a framework.

KATHRYN KLEIMAN: (off microphone).

This could be different types of standards for accreditation.

CHRIS DISSPAIN: And that's a very fair point and goes back to the point about what work -- what other work needs to be -- to be done either in the policy development process itself or before GNSO starts a policy development process.

ROD RASMUSSEN: And just to follow up on that, what we've proposed here is to try and take advantage of existing systems and existing protocols for deconflicting these exact types of issues that are already out there, that are already being used. One of the things we found out by doing this work -- and I learned a lot about how law enforcement works and I thought I knew quite a bit -- is that there are a lot more systems, a lot more accreditation schemes, a lot more providers of these kinds of services.

And the frameworks within which to operate them have been in existence for years and decades that we can take advantage of for doing something as simple as WHOIS lookups.

SUSAN KAWAGUCHI: Just one point I wanted to add to that, is, you know, we gave a lot of thought about the I.P. address. Is that included in this? That's tracked

by the registrars. Should we -- should that be a data element included in the new data that's provided for a domain registration and we decided collectively no.

But really an I.P. address might get you to that person you are looking for much quicker than a gated data record with a proxy registration that -- you know, I mean, you could put lots of layers. And if you do know that you are one of those people making statements that you're going to be targeted, then the secure protected credential.

So, you know, I think we did give it a lot of deep thought. Is it perfect? Probably not. I don't know what is perfect.

But we are also looking for that community input, not "we," but the community will look for that input as this goes out to whatever PDP structure. And so these are high-level principles to guide the community because we've had the luxury of really thinking deep about this. But then the community, you, Kathy, needs to be there to put -- to make sure the implementation of this process, if it's decided, goes in the direction that's safest for the community.

KATHRYN KLEIMAN: I'm still on the high-level principles and asking questions about them. So let me go back to my original question, which was, first, I've got two reports here. One is the interim report. That was about, what, 84 pages or so; and the final report which is double that length. So if you see people looking confused, it is a lot of material that came.

CHRIS DISSPAIN: It is a larger font.

[Laughter]

KATHRYN KLEIMAN: It is a lot of material.

MICHELE NEYLON: Please ignore Chris.

KATHRYN KLEIMAN: A lot of material to absorb and kind of wondering how we go from a draft to a final with so much more detail. Let me ask about one of the details, and then I will back in line to ask about others. It has to do with the contacts.

Let me flip over here.

What contacts are mandatory, what contacts are optional? When we talked -- in Singapore, we talked about optional contacts that were being added because large companies wanted them. Large companies did not want their technical contact contacted about abuse. They didn't want their abuse contact contacted about legal matters.

But to impose all of those contacts on every registrant seems extreme. Even with the consolidated centralized database we've talked about from the beginning, it should be streamlined and narrower, not massively expanded.

CHRIS DISSPAIN: But surely you could just go -- I mean, we do this in Australia. Surely, you just go -- I'm a small business. It is just me. I will fill every box.

KATHRYN KLEIMAN: Chris, "legal contact" means something and it assumes something. When we use it in the United States, it assumes you've got an expert and every registrant may not be that expert.

CHRIS DISSPAIN: Okay. So I accept -- I accept that -- I accept that the term --

KATHRYN KLEIMAN: It is a mandatory field, Susan. And it is public.

MICHELE NEYLON: She's not disagreeing with you.

(multiple speakers).

CHRIS DISSPAIN: Just listen. We acknowledge it is public. Not a problem. I also acknowledge that it may be -- in certain jurisdictions, the term "legal contact," may have -- may have --

KATHRYN KLEIMAN: Very specific.

CHRIS DISSPAIN: -- may have a specific meaning and that's fine.

The point is, what it's meant to be is the contact -- if somebody comes into the system, goes through all of the hoops, et cetera, and has -- and has designated the purpose they are looking for the data is because it's a legal issue, they would be given the legal contact. What that enables my business to do is to designate, should I wish to do so, that my lawyer is listed in legal contact.

It is equally possible as a small business, as we do all the time in the box-ticking exercises, that we go through that I might put myself in every single box. The same as you do right now. You go to WHOIS lookup right now. You will see a lot of the individuals they are the tech contact. They are the admin contact. They are every contact.

Is the problem that it's called a "legal contact" or is the problem that I have to fill it in? What's the --

KATHRYN KLEIMAN: First, box-ticking exercises are very dangerous. And.

Second, legal contacts mean things.

But, third, let me get to my real concern, which is that when you look at legal-based contacts, you have at least -- I'm looking at page 52 of 166. It has the name, the street address, the country, the phone number all mandatory, all public.

CHRIS DISSPAIN: No. No.

KATHRYN KLEIMAN: And that's -- so at least that's how I see it because I have the --

JEAN-FRANCOIS BARIL: I think, Kathy, this is part of the confusion that Stephanie was mentioning before.

KATHRYN KLEIMAN: Can I just finish my sentence and, please, I would love to hear your response. If this is mandatory and public, first, it is a huge change from the interim report. And, second, it is very dangerous because it looks as if the registrant would have -- it looks as if the only group that's left with protection is corporations.

CHRIS DISSPAIN: That's not correct.

KATHRYN KLEIMAN: Let me listen to Jean-Francois because I --

JEAN-FRANCOIS BARIL: Yeah. And I think we are very pleased that you asked this question because this has been in the corridor many times the question to me and to every one of us, and this one, it is written onto this one. It is of course not perfect things but it is part of what we just mentioned before with Stephanie on the sometimes misleading wording that we put into this one. This will be clarified, but let's -- let me --

KATHRYN KLEIMAN: So will you be changing page --

SUSAN KAWAGUCHI: No. Let me talk first.

So there is data that could be public through purpose-driven -- you know, I mean, you have to go in, you have to ask for it based on a specific purpose.

So that -- those elements, those data elements, could become public at any time.

>> (off microphone.)

SUSAN KAWAGUCHI: And disclosed. Yes. Like -- okay. Sorry.

>> (off microphone.)

SUSAN KAWAGUCHI: So they're disclosed. But it would become available to the -- to an individual third party, and so -- but there are also data elements that we're recommending collecting that are discretionary, so those are only disclosed if the -- the registrant agrees to that.

So there's sort of three levels of data. Do I think this report is absolutely clear? No.

Do I think we did a really good job in trying to make sure that people would know that this data they are providing could be disclosed --

>> (off microphone.)

SUSAN KAWAGUCHI: Yeah. It took me a while to get there.

ROD RASMUSSEN: Yeah. No, I was talking about the --

SUSAN KAWAGUCHI: Oh, okay. So --

CHRIS DISSPAIN: So Kathy? Kathy?

KATHRYN KLEIMAN: Uh-huh.

CHRIS DISSPAIN: Okay. That is the -- that is what is publicly disclosed. Publicly disclosed.

>> (off microphone.)

CHRIS DISSPAIN: So let's be clear.

KATHRYN KLEIMAN: Will you be editing Page 52?

SUSAN KAWAGUCHI: No.

>> (off microphone.)

KATHRYN KLEIMAN: It says coupling, and it said optional and gated in the interim report, which was a lot clearer.

ROD RASMUSSEN: So this is a process question. This is a process --

Are we going to edit Page 52? The report is published, right? We will add addendums, explanations, et cetera, for it -- to clarify these kinds of issues, and there's many of them that are in lots of spaces, where this kind of -- exactly this dialogue, "What do you mean by this, how does this work," because there are -- it is in there and if different principles are -- point to how this works, whether it's public or not --

KATHRYN KLEIMAN: Because it looks like you're undercutting the process that you --

>> (off microphone.)

ROD RASMUSSEN: Right. We totally get that, we understand that, and we're going to put out a clarification around this, so that it is clear to you and everybody else that has this issue, which has been brought up by many.

>> (off microphone.)

CHRIS DISSPAIN: -- I need you to understand that we are very, very clear. That is the open -- open public, if you want to call it public, data.

>> (off microphone.)

CHRIS DISSPAIN: Anonymous, yes. Sorry. Outside -- outside of the gate. Outside of the gate. Now, is it mandatory to have -- to provide a lump of data? Because you used two words. You said "mandatory" and "public."

KATHRYN KLEIMAN: Right.

CHRIS DISSPAIN: Yes, it is mandatory. However -- well, subject to proxy and stuff.

But if that page -- and I haven't looked at that page for a while. If that page gives you an indication -- gives you the impression that your address would be displayed publicly --

KATHRYN KLEIMAN: Right.

CHRIS DISSPAIN: -- the answer is: It will not. And there are -- and we will ensure that there is clarification so that you are comfortable that that is the case.

KATHRYN KLEIMAN: I would appreciate that. Thank you.

CHRIS DISSPAIN: Thank you. Okay. Good.

WENDY SELTZER: Thank you. Wendy Seltzer, here speaking with some high-level questions and some very detailed questions, taking the opportunity of having the panel in front of me to answer some questions that I haven't yet been able to parse, reading this 160-plus-page report.

The high-level question is: Did the group discuss that, you know, what this report does fundamentally changes the nature of domain name

ownership? It imposes new accountability requirements on the owner of a domain name that make it impossible simply to have a domain name for the purpose of having a stable location for on-line speech and a DNSSEC signature in the root -- key in the root, rather, through which they can secure communications, and instead adds additional information that every user must supply as a condition of domain name ownership?

MICHELE NEYLON: Wendy, you've registered domains, haven't you?

WENDY SELTZER: Yes.

MICHELE NEYLON: Okay. You are subject to the registration agreement you have with your registrar and also subject to the UDRP. There's a degree of accountability at the moment.

WENDY SELTZER: Yes. I believe that's different from --

MICHELE NEYLON: No, no. Hold on. No, no. Please. Hold on.

There's accountability now. It's just not as clear. I don't -- I don't think there's -- that it's -- I don't see this as being a seismic shift. I mean, it might be clearer and easier for people to understand that there's a

degree of accountability, but if I go off and I register a domain name now and infringe on somebody's trademark or something like that, I could lose the domain, be that via URS or UDRP.

If I go off and I register a domain name and I use that solely for the purpose of distribution of malware or something like that, the domain name could be pulled at either the registry level or the registrar level. There is accountability --

WENDY SELTZER: And I'm not -- thanks. And I'm not suggesting that any of those --

MICHELE NEYLON: No, but that's -- but --

WENDY SELTZER: But the accountability doesn't hinge on the registration of the domain name or misuses -- or misuses either in the registration or use of the name, but not in the holding of a non-infringing name itself.

MICHELE NEYLON: I'm not sure I'm --

>> (off microphone.)

FABRICIO VAYRA: So Wendy, if I could just add to what Michele said, I agree that we actually amped up accountability a lot, but actually for those who hold, display, disperse, transfer, seek data, I don't think there was a seismic shift in those who register domains because just to add to Michele -- at least I didn't see it so hopefully I'm not speaking outside of turn because when I've registered a domain -- I'm assuming you saw the same registration agreement which says specifically in a clause that you agree to put accurate data, and then in the UDRP it actually has accompanying clauses. And as a matter of fact it's one of the reasons under every TOS I've ever seen in 14 years that says your domain name can be suspended or deleted at the discretion of the registrar for putting in inaccurate data.

So when we amped up accountability for all of those people seeking that data that's supposed to be accurate, we didn't think we were doing a seismic shift for the registrant, because the registrant already under that obligation.

>> (off microphone.)

MICHELE NEYLON: Sorry, Wendy.

I mean, if you want to -- if you can explain to me a little bit better what you see as being significantly different, I mean, I'd love to -- I really would like to know. It's just --

CHRIS DISSPAIN: So maybe let Wendy try and do that.

MICHELE NEYLON: I mean, I'm just a little bit confused. I mean, if there is something that we have done that gives the impression that we've put some massive change, please, I'd love to -- I really would like to know. But I think all we've really done is -- is highlighted the concept of there being accountability, which was already there but maybe it wasn't being enforced. I don't know.

WENDY SELTZER: I think you've required additional data elements, you've required validation of data elements, not just the input of accurate data elements, and you've imposed some of that accountability on the domain ownership, as opposed to domain use or display of a string that infringes a trademark.

CHRIS DISSPAIN: I'm not sure that -- I'm not sure there are any additional data elements.

>> (off microphone.)

CHRIS DISSPAIN: I'm sorry. They might be additional in the sense of you didn't -- you weren't asked to ask a legal contact before but if you just look at the actual data elements, there aren't any additional ones, and if validation --

>> (off microphone.)

CHRIS DISSPAIN: Sorry?

MICHELE NEYLON: That are required.

CHRIS DISSPAIN: That are required.

MICHELE NEYLON: There are plenty of optional ones we put in.

CHRIS DISSPAIN: Yes. And then the validation doesn't really change --

WENDY SELTZER: It changes the cost. It changes the cost of providing the service and, therefore, the cost of the service that will likely be provided.

>> (off microphone.)

FABRICIO VAYRA: Yeah. I -- listen, I think that that's a great point of discussion. I mean, in the year and a half that we brought in vendor after vendor after vendor after vendor, not one of them actually made that point, and that's a very valid point that you're bringing up, so I'd love to see the data on that so that we can actually put it into the PDP process or the discussion. Because the one thing we tried very much to avoid and why we have 166 pages, why we put in 180 principles, why I spent personally a year and a half of my life traveling around the world, was to make sure that we tried to unturn every stone and actually not base anything here on assumptions.

And so I think it's very dangerous to try to assume those things without the backing data. So if you have it, please give it to us so we can incorporate it through the process.

WENDY SELTZER: I've been at plenty of earlier public forums where the costs of validation were discussed, so I imagine some of you were as well.

CHRIS DISSPAIN: Okay.

MICHELE NEYLON: Sorry. Just to add to this, I mean, I -- I don't disagree with you that there is a cost of validation. I'm a registrar. I'm very aware of that.

Unfortunately, the 2013 RAA introduced some verification, and then there's also the validation which hasn't been fully implemented yet.

Now, if we can make that all go away completely, as with my contract, I probably wouldn't be complaining about it, but, you know, the reality is it's there.

We did have discussions with -- with several companies looking at some of the validation and, you know, the costs associated with that, and, you know, the thing I think is that some of the costs exist in the system now. Some of the costs are borne by the registrars, some costs are borne by the registries, some costs are borne by third parties.

So at the moment, there are costs there all over the place.

Dealing with the WHOIS accuracy complaint costs me time and money. If that went away, I would be quite happy. And I'm only dealing with a very small volume of them.

CHRIS DISSPAIN: Just very quickly, Rod, because Wendy I know has other things she wants to talk about, so let's --

ROD RASMUSSEN: Yeah. I'd just point out that we had proposals or discussions with UPU and the Secure Domain Foundation. The Secure Domain Foundation is offering validation for free, so I don't know how you can get lower cost than that to registrars.

And then the other thing is the concept of the validators in theory should lower cost because you could actually localize that. So if I'm GoDaddy or what have you or any registrar in any country, I can now use a validator that's in a third -- you know, in a country where I don't

have people that speak that language or know the guy who lives in that place over here actually is that person or what have you and that should lower costs by introducing more ability -- more ways to do the validation than currently exists.

CHRIS DISSPAIN: Wendy?

WENDY SELTZER: All right. I'll be brief in additional comments.

You make reference to a privacy policy and risk analysis, both of which are recommended and I very much look forward to seeing those done before all of this collection infrastructure is built.

CHRIS DISSPAIN: So we've asked the GNSO to give us a list, so make sure you get those put on the list. Perfectly fine.

WENDY SELTZER: And finally, one of the -- the technical questions that occurs to me, reading this: Can a registrant have a distinct ID for each place his contact appears, even if it's the same contact data?

CHRIS DISSPAIN: Do you mean if I choose to put my name into the legal contact and the tech contact, can I have two separate IDs?

WENDY SELTZER: Yes.

CHRIS DISSPAIN: Yes. I would --

LANRE AJAYI: Yes. You can choose to have multiple contact IDs. That's up to you.

WENDY SELTZER: But every piece of information is the same, yet it gets a different ID number every place it appears? Is that --

MICHELE NEYLON: I think you have the choice -- I think you have the choice, Wendy. I mean, if you want to -- I think I know where you're coming from, and your concern would be that by reverse-engineering the ID, you can work our patterns, et cetera, et cetera.

CHRIS DISSPAIN: Yes.

MICHELE NEYLON: So if you want to create multiple IDs for yourself, I don't think there's any real issue with that.

The -- the thing is that for -- let's say for my company, we have domains registered. I would prefer to be able to just have, you know, one ID because it's not like I have a staff of millions.

CHRIS DISSPAIN: (off microphone.)

MICHELE NEYLON: So there's no reason why you wouldn't be able to have multiple. It's not an issue.

WENDY SELTZER: Thank you. I appreciate that.

CHRIS DISSPAIN: Much like personalities, Wendy. As many as you want.

Rob.

ROB GOLDING: Hi. Rob Golding from Astutium. We're a registrar.

I'm particularly looking forward to reading Stephanie's blog. I'm concerned about you now having a domain name, though. You're here at ICANN. You're, you know, on the panel. I know now where you live. I can go and borrow that 50-inch plasma TV that you've got while you're in London.

So hopefully you've taken some sort of privacy protection on that and hidden that data.

I have waded through the original interim report and part of the final report and I have similar questions to an earlier one.

It isn't very clear what is mandatory, what is optional, what is declared, what is not declared, what "public" really means.

Is there going to be a final -- final, final version of that which is a lot clearer?

CHRIS DISSPAIN: (off microphone.)

ROB GOLDING: Because we have to know what to supply, we have to know what we get permission from our customers for.

CHRIS DISSPAIN: So let's be really clear. First of all, this is a report and it's not -- it's not policy; it's just a report.

Secondly, if we receive feedback, which we have done, that something is unclear, we will fix it.

Whether we choose to fix it by republishing the report or putting -- it doesn't much matter for the sake of discussion. What matters is, it will be fixed.

MICHELE NEYLON: Just speaking here, Rob, if it's, you know, something like that, maybe some kind of matrix-type thing might work. I mean, the thing I think around this is we put -- the feedback we got from interim stuff that we published and sessions was, you know -- you know, "Give us more

detail, give us more detail," which is part of the reason why it went from, what is it, 88-page odds to 166. No, Kathy, it wasn't a big conspiracy to upset you. Honest.

Maybe adding some kind of matrix or something like that which would make it clearer. Personally I'm all for that. I mean, some of the feedback we've had from people to date has been, you know, there's a certain lack of clarity. And that wasn't intentional. That was more just if you've been eating, sleeping, drinking, probably having nightmares and dreams about this stuff, it might be a bit hard to, you know, kind of distance yourself enough to realize that it wasn't a hundred percent clear to others.

>> (off microphone.)

ROB GOLDING: Yeah. There were comments earlier regarding commercial use of the data, particularly around people like DomainTools --

CHRIS DISSPAIN: Yeah.

ROB GOLDING: -- who aggregate the only two decentralized gTLDs. They're mostly centralized anyway.

What provisions are in there, if at all, for recompensing the registrants for their personal data?

People aren't currently used to exchanging their name and address in order for free use of Facebook. They understand that their personal data -- and it is protected under U.K. law, we're in the U.K. -- has a value.

CHRIS DISSPAIN: Yes.

ROB GOLDING: What payments are going to be made for registrants who choose to allow their data in this system?

CHRIS DISSPAIN: I'm -- I'm sorry, I don't -- I actually genuinely don't understand the question.

You -- you enter into a bargain where you go to -- you go to buy -- you go to buy a domain name and then --

ROB GOLDING: Yeah.

CHRIS DISSPAIN: -- there's a series of systems and rules in place in respect to the data. That is declared. There's -- there's governing law.

I'm not -- I don't understand what you're --

ROB GOLDING: You're --

CHRIS DISSPAIN: Are you suggesting that the data would be sold?

ROB GOLDING: Well, you're -- one of the suggestions is that commercial entities -- let's just pick on DomainTools just because we know --

CHRIS DISSPAIN: I don't think we're -- I mean were we talking about --

ROB GOLDING: Are you going to mine this data or re-present this data --

CHRIS DISSPAIN: Are we talking about selling the data? I'm not sure.

MICHELE NEYLON: What he's talking about, I believe -- and I mean, sorry, Rob.

CHRIS DISSPAIN: (off microphone.)

MICHELE NEYLON: Sorry. I'm used to exchanges with Rob, so I'm kind of -- I kind of speak semi-fluent Rob Golding.

I think what Rob is talking about is third-party access --

ROB GOLDING: Yeah.

MICHELE NEYLON: -- third-party bulk access to data in order for services such as DomainTools to exist. I think that's all he's asking about.

ROB GOLDING: Or the solicitor earlier who provides reports to his customers about infringement and things like that.

MICHELE NEYLON: Yeah. My --

ROB GOLDING: My address has a value. Tesco's will pay me 27 pounds per year to know where I am.

CHRIS DISSPAIN: Yes. But I don't need to go to Tesco's to find your address right now.

ROB GOLDING: You don't. You can --

CHRIS DISSPAIN: I can go to WHOIS, and assuming that you've --

ROB GOLDING: If I choose to allow you --

CHRIS DISSPAIN: -- if you have actually -- well, no. Assuming you've complied with the terms of your contract, actually.

ROB GOLDING: I have. I have I've listed an address. You can post a --

CHRIS DISSPAIN: Exactly.

ROB GOLDING: Not my address.

CHRIS DISSPAIN: Fair enough. But isn't that the point?

>> (off microphone.)

MICHELE NEYLON: I think -- all right. Chris, I think Fabricio -- or was it Rod? Somebody -- the access?

>> (off microphone.)

MICHELE NEYLON: For DomainTools and other companies.

>> (off microphone.)

ROD RASMUSSEN: No. It's in the report. Number 50, I think, was the number.

SUSAN KAWAGUCHI: Yeah. Uh-huh.

ROD RASMUSSEN: And the key there is that if you had third-party access to the data of any sort, it would still have to fall under the same principles around how it's treated, how it's -- how it's accessed. It has to be done carefully, and that you wouldn't have bulk access so the people could go spam you or whatever the heck they've been doing for the last 10, 15 years with this stuff.

So we carved out a way for that to occur. How that actually gets written up and enforced is a part of the -- part of the policy development that has to go forward.

CHRIS DISSPAIN: I think that's right. I'll come to you in a second.

I think there's a dichotomy between the current situation, which is that -- that the -- those businesses exist because they have open access to the -- to the data, and you're put to inconvenience in order to not have the -- the real -- not -- not "real," but you know what I mean -- data out there.

And what we're talking about, which is effectively turning that on its -- on its head but still trying to find a way of enabling those -- those sorts of things -- those innovative -- let's call them innovative things to happen.

That's not -- we haven't done that. We have not specifically said how that should be. What we've said is, the community should think about whether it is a permissible use to have bulk -- to have that access. Yes, Fab, you can -- Stephanie, I know you want to come in.

FABRICIO VAYRA: Sorry, Stephanie. I don't mean to jump on.

>> (off microphone.)

FABRICIO VAYRA: I just want to say in conjunction, we said would the community consider and evaluate this.

Please do, when you consider this, that one of the reasons we've left it the way it is in the report is that I don't want to -- you know, I personally and I'm sure the group does not want to promise you or Milton or

anybody else certain layers of systematically applied privacy and data protection rules and then allow somebody into the system that then makes a carbon copy of that data and loopholes everything we worked hard to do and then violates that.

So in essence, you may think you're entering a system where you say, "I've been protected. There's accountability. People who access my data, it's purpose-driven, they -- you know, there are all these checks and balances," and somebody goes into the system, pulls all the data, and then sells it.

And they're going to sell it without any of those things that the community has bargained for so hard to protect people.

And so that's why we were cautious. Again, we realized those data -- that those services are out there. Hell, I have a subscription, through my company, to about two or three of them. So we don't -- we're not trying to kill an ecosystem, but we also want to make sure that everyone's fought for on privacy and data protection isn't circumvented.

CHRIS DISSPAIN: Stephanie, I apologize for leaving you out.

STEPHANIE PERRIN: Some of these practices even if they're longstanding and been around for 20 years would not be permitted under data protection law which is why the data protection policy has to be done first so that you can set the parameters because a permissible purpose for some purposes may

not be permissible as far as you're concerned as someone who has data protection rights.

CHRIS DISSPAIN: Sure. It comes back to your rules to the engine again, for the different people protected in different ways. One more go.

ROB GOLDING: I know Canada has reasonable privacy rules for individuals. I know islands are covered by the general E.U. In the U.K., certain information is considered to be private and you can --

STEPHANIE PERRIN: And you sound like a potential guest blogger, I have to say.

CHRIS DISSPAIN: Now we're building a whole new Stephanie ecosystem. It is enough.

ROB GOLDING: I have to deal with registrants and ask them to update their WHOIS if we get a complaint. Thankfully we don't generally get many because as a registrar, we know who our customers are. In fact, as far as my personal opinion is, is that WHOIS should just be turned off because the only people who need to know who the registration is for are the registrars.

But the overwhelming response I've had from existing registrants registering new TLDs and gTLDs is why do they have to put their data out in the public anyway.

CHRIS DISSPAIN: I agree. Exactly the same in Australia.

ROB GOLDING: Just a stat for the panel, since we made protection as a free service on all domains, simply because we want people to have the option, we've had three out over 900 people turn it off and say they want their details public. Three out of 900 in the last week.

CHRIS DISSPAIN: Thank you very much.

MILTON MUELLER: Hello. Milton Mueller here, Syracuse University, Internet Governance Project. I have two questions for you, assuming I can get to them without being interrupted by the moderator.

CHRIS DISSPAIN: Thanks for the rhetoric, Milton.

MICHELE NEYLON: If you want, we can take the microphone off the moderator.

MILTON MUELLER: I think he should just put it down so he has to actually reach for it before he can intervene.

Now, my first question is very fundamental. Just assume I'm an ordinary individual domain name registrant. I don't have a company. I'm concerned about my privacy. Under the current system, if I'm concerned, I either hire a registrar like the one he just described that gives me some protection or I hire a proxy service. And if law enforcement needs to get behind that, they have some procedures for doing so.

Tell me what your system -- how your system makes my life better. Just my life. Not the trademark lawyers, not the law enforcement, just my life.

CHRIS DISSPAIN: As a registrant?

MILTON MUELLER: As a registrant.

LANYRE AJAYI: Under the processes you just mentioned in existence in the present are this, the proxy service providers are still there. You can still use it. And there are purpose-based contacts, an option for you if you want to use. If you don't want to use, it's okay. Use your name as default.

So to me, your life is much better now because you have more options, including the existing --

MILTON MUELLER: What are the options?

FABRICIO VAYRA: My team oversees the domain registrations for Time Warner. Time Warner has multiple entities. At one point, we had I think 65-, 70,000 domain names. It is a little hard to manage.

How does that make my life easier? One, when I go to register, I'm given options as to what I put in. I no longer have to have my name, my address, my email address, et cetera, and then create a roll account and then devise a technical account because it all went to one person, right? That one person can just put their information in and they are done.

On top of it, once they proceed out of there, you do have privacy proxy. You can hire a registrar to do your stuff. But the reality is I have entered the information once, I can update it once, I can port it once like a phone number.

So me as a registrant who had to manage 70,000 domain names, my life is much, much easier.

For the simple user who has one or two like myself as a person who uses privacy proxy for all the reasons you would think, my life is easier again because I put it in the one time and then I do the check-box exercise we talked about with Kathy where I say "I want privacy proxy." Check, check, check. I have been informed for all the purposes for which I might disclose that data: Legal purposes, what have you.

I say domains by proxy, check, check, check. The only thing that gets published outside are details relating to domains by proxy. It becomes a much easier system to manage from a management perspective.

And it doesn't change, though, the ecosystem of what you're talking about with privacy proxy, capability of having a registrar do things. It shouldn't change the cost model with that perspective either.

ROD RASMUSSEN: Just one quick point as well. Me as an individual in the current system, I don't necessarily know how to designate something that I might not want to get bothered by. I would still get bothered by it by the proxy solution if they just forward the email to me, right? I can say for technical or abuse matters, Hey, GoDaddy is handling that for me and they are offering it as a service or whatever registrar. I can actually hand off some of the things that currently I may get bothered by and I don't want to deal with it even as just an individual domain holder.

FABRICIO VAYRA: It becomes much more transparent to someone, in particular the kind of first comer at least the way we are envisioning it. Obviously, there is some implementation it has to go through from the registrar to customer. We honestly wanted it to be a lot more transparent to what it was you were, one, putting data in for and what that could be used for.

And so, you know, I remember with Scott, we had a conference call, I don't know, a year ago where he was talking about he finds it a real pain in the butt when he has to go in and put in data for a registrant, data for

an admin, data for a tech, and it was like, why do I have to go through that exercise? Now you don't.

MILTON MUELLER: Basically, for an individual registering one name, there is not much of a difference. For multiple domains, it gets a little more efficient and so on. That's all I want to hear about that because I have another question that's actually more relevant to developing your report or policy out of your report.

MICHELE NEYLON: Sorry, Milton. Do you mind if I just add one thing with respect to your individual registrant thing? One thing that the system -- there's a couple of things the system does have that I think from a privacy perspective are a little bit more interesting.

The idea of this rules engine that depending on which jurisdiction you're in, you would get different levels of privacy protection. I think that's quite interesting. I mean, the devil is in the details, and --

MILTON MUELLER: This sounds like hand waving to me. I deliberately did not bring that up, the rules engine. Yeah, we will put all the rules of the world in an engine and it will magically protect you.

MICHELE NEYLON: I think the idea, I think, isn't a bad one. In implementing it, I suspect, it is going to be a lot more complicated.

MILTON MUELLER: Yes.

MICHELE NEYLON: Ultimately, as we all know, at the moment there's a lot going on in this entire space around privacy, particularly here in Europe. So what is going to be required of us or not required of us as companies and as individuals over the next couple years are going to change quite a bit.

If you look at the public data example, which I think is the one up on the screen at the moment, that's significantly less data that's being shared outside any kind of gate than is the current status.

I mean, if you do a lookup on any .ORG or .COM, you get a hell of a lot more information. So I think in some respects, it would be a significant improvement.

Obviously, you know, you still have a lot of options open to you, be that using privacy proxy, different services from different companies, individuals, whatever. I mean, you still got all those options.

CHRIS DISSPAIN: I know Stephanie wants to comment. Just quickly Stephanie, and then Milton's second question.

STEPHANIE PERRIN: I was just going to respond to Milton, that if -- your choice is to either move out of New York State or assign your very best post doc to work on the privacy policy working group so THAT it is harmonized at a high-

level because sadly everything Michele talked about wouldn't really apply to you.

MILTON MUELLER: Okay.

So if you could put the slide about purposes up there, I don't know if that's hard to find.

CHRIS DISSPAIN: Prescribed purposes.

MILTON MUELLER: It might be useful. So I was really --

CHRIS DISSPAIN: That one?

MILTON MUELLER: Yeah. My understanding, your process was somebody is authorized to search the database and surveil people for specific purposes. And then when they make a query, they tell the system what that purpose is, and the purpose matches it against their accreditation and then they're allowed or not allowed access to the data. This sounds to me -- I mean, absurdly simple to lie to.

I say I'm looking for trademark protection, I'm a trademark lawyer. Maybe I really am, but I'm actually looking for an old girlfriend's domain name registration. And I tell it -- you know, I'm smart enough that when

it asks me what my purpose is, I tell it the wrong purpose. How do you know what I'm really doing?

CHRIS DISSPAIN: How are we dealing?

Go ahead. Faisal?

FAISAL SHAH: I can see what you are saying. That's why we have audits in place. One of the things we talked about was the ability to put in behavioral analysis and pattern analytical tools to be able to figure out if somebody is actually -- what are they doing? They say they got this purpose. They are doing something completely different. They say -- you know, there's going to be a UDRP and suddenly they are just fishing around or whatever.

To some extent, that is something that we've tried to address with some of these other features and mechanisms within the system to be able to capture that and then pull that in and do something about it within the RDS.

MILTON MUELLER: In terms of implementation, you're saying that's something you would like to do but really you don't know how. And in terms of policy, that would be something to pay very careful attention to.

(multiple speakers).

CHRIS DISSPAIN: (off microphone.) I can speak from experience in Australia. We have certain policies that require you as the person asking us for information to warrant certain things to us.

Now, obviously I couldn't say to you that a person hasn't miswarranted. But I can tell you that we pick up patterns quite easily and so a single use -- a single misuse, for want of a better term, because you are trying to find your exgirlfriend, I might not pick up. But for a continuing use for a purpose would be a lot easier to pick up.

LANRE AJAYI: In addition to that, the system makes provision for auditing. During the auditing process, you can be found out and consequences for misbehaviors.

CHRIS DISSPAIN: I think it is also fair to say that you can proxy -- you can proxy behind a heap of stuff. Sorry. You can go behind a proxy for a lot of these purposes. And so, therefore -- it becomes a narrower, narrower, and narrower funnel if you choose to use the proxy services that your real information is available. In fact, it may not be at all.

ROD RASMUSSEN: It is a r-back (phonetic) system, right? None of them are 100% going to guarantee that insiders can -- won't abuse them. That will happen. That happens all the time with people and government officials looking up exgirlfriends and all that stuff. It does.

What we are trying to do is create a way for you to actually figure that out, which you can't do at all today. I can go look up my exgirlfriend's domain names today with the fully available, anonymous, nobody-is-tracking-anything system that there is.

At the end of the day, what we want to do is create a system where you can start enforcing some of those things that you're concerned about and then have penalties obviously, sanctions, et cetera, for people who abuse that system so they're denied access or report it to the authorities, what have you. If that's stalking, in some country that might end up leading to a prosecution.

FABRICIO VAYRA: I would add, to summarize what Rod and what everyone is saying is that back to the basic question we were asked: Is there a better alternative? And we said the resounding answer is yes. The question wasn't: Is there a perfect alternative? The reality is there just isn't.

I totally get your point. I think to the extent that we can get input to try to correct those things -- that's what we're honestly trying to get at, right? We're relying on the fact that if someone at my company uses our token, they're going to realize if they go look up their girlfriend and that girlfriend realizes that information was obtained via the Time Warner token through the WHOIS, they're likely going to get fired because when our token searching turns off a legitimate merger acquisition, asset management, et cetera -- at the end of the day, we're relying on an accountability structure hopefully to blanket over the gaps that -- you know, as Rod was saying, we just can't build -- I mean, we

don't know it. If we knew it, we'd put it out there. There is not a perfect answer to that.

MILTON MUELLER: I think the dilemma is, you are creating this enormous, global, centralized surveillance system. You are legitimately trying to build accountability and privacy protections into it; but at the same time, one has to question whether you should build the tool at all and whether we actually need that tool and whether it is worth the risks and the costs.

FABRICIO VAYRA: Look, in the times --

CHRIS DISSPAIN: Hang on. Thank you, Milton.

The scribes are asking if we could make sure to say who is -- make sure you say your name before you speak.

FABRICIO VAYRA: Fabricio Vayra.

The point of surveillance and aggregated, disaggregated, and all these discussions, we've talked about it a bunch.

And, you know, when we hear the argument that aggregated is going to be much easier to crack and go in and get information from, you got to look at the fact that what we are arguing are is in the system where the problem already occurred in a disaggregated model. Because last I

checked, Microsoft, Yahoo!, Google, et cetera, are actually different companies not under the same umbrella. And they themselves have disaggregated servers.

What we were hoping -- and maybe it is the wrong answer. What we were hoping is in an aggregated model where you can actually systematically apply tougher rules, tougher security, tougher privacy, tougher data protection rules, then it becomes tougher for people to crack that system as opposed to a system today where it's just -- all you need is one weak link that then undoes the entire system of disaggregated models. That was our attempt. Maybe we got it wrong, but that was our attempt.

CHRIS DISSPAIN: Very quickly, Carlton, because we have --

CARLTON SAMUELS: Yes, I wanted to -- this is Carlton for the record. I wanted to address the issue.

If we believe that for surveillance purposes you really have to get into the database to surveil, I think that's wrong. All you have to do is sit outside the gate. You don't have to be inside to surveil.

And the surveillance issue is really a red herring. We always seem to forget that there's an infrastructure for this, huge infrastructure everywhere, hundreds of billions of dollars. They didn't put all that money in just to sit as a white elephant.

And I don't believe you're going to get away from somebody sitting on the ramp, off the ramp, on the highway and listening and watching. Thanks.

CHRIS DISSPAIN: Thank you. Okay. Sir?

KEVIN McARTHUR: I'm Kevin McArthur. I'm with the CIRA board, .CA operator. We are one of the registries that has actually done WHOIS privacy for individual registrants. And some of the challenges that we've had in doing that is the security of that information.

So my question is: Under what legal regime will the actual rules engine, the database, all that stuff operate? If it fails, who do I file suit with?

CHRIS DISSPAIN: No one, because you shouldn't be allowed to.

[Laughter]

So it is a function -- to some extent, it is a function of the country that you're in.

KEVIN McARTHUR: Well, no. This system has to exist somewhere.

CHRIS DISSPAIN: I'm sorry. You mean where will we put it? I apologize. I misunderstood.

We don't -- we haven't -- sorry, Poland? Oh, the moon. Yes. There you go.

I mean, the answer is we don't yet -- we have not made a recommendation of place, although I'm sure that Jean-Francois would like to run it from his house.

ROD RASMUSSEN: We have principles actually. It should be established in an area with high data protection written in the law and we said something about the law enforcement.

CHRIS DISSPAIN: Yeah, we have.

ROD RASMUSSEN: Trusted law enforcement. Trusted law enforcement.

(multiple speakers.)

CHRIS DISSPAIN: -- better than it is now because right now what would the answer to the question be?

KEVIN McARTHUR: In the Canadian context, the answer is we keep our registrant data private.

CHRIS DISSPAIN: In a gTLD world, what would the answer be? This doesn't affect .CA. What would it be in a gTLD world right now?

KEVIN McARTHUR: Some of these domain names have not yet been approved in the new gTLD space so we don't know what the data protection regime will be for those new gTLDs.

CHRIS DISSPAIN: My point is, where would you -- your question is who would I sue?

KEVIN McARTHUR: If I'm in .TORONTO or .QUEBEC and one of the new gTLDs affecting Canada and the registrant's privacy is violated through failure of the rules engine or through legal issues related to the jurisdiction in which the rules engine is operating, who do I have redress with?

CHRIS DISSPAIN: So -- I accept the question. And we've got a series of principles as to where the RDS should be located. But you still have the issue of where's -- irrespective of the RDS, you still have the question: Where is your registrar? Where is your registry? And where's the registrant?

KEVIN McARTHUR: This is my question. Where does that jurisdiction question --

CHRIS DISSPAIN: Well, it depends on all of those things.

FABRICIO VAYRA: So what we tried to do was --

CHRIS DISSPAIN: Fab and then Carlton.

FABRICIO VAYRA: -- was create a rules engine that actually accounts up- and downstream for the jurisdiction of the data subject.

So I can understand why you're talking about where the RDS actually sits, but hopefully it -- it kind of assuages those concerns knowing that what we're really trying to implement is not based on where the data sits but who the data subject is and where they sit.

So if I'm doing a search from, say, the U.S. to Canada, the rules engine would actually apply the laws, the privacy and data protection laws, of your jurisdiction, so that I don't get data that I'm not supposed to get only -- merely because I'm searching from outside your jurisdiction.

KEVIN McARTHUR: (off microphone.)

FABRICIO VAYRA: And again, that --

KEVIN McARTHUR: (off microphone.)

CHRIS DISSPAIN: But ICANN's not in control of the data, though.

KEVIN McARTHUR: Pardon?

CHRIS DISSPAIN: ICANN doesn't control the data.

KEVIN McARTHUR: It controls the rules engine.

CHRIS DISSPAIN: No.

KEVIN McARTHUR: No?

CHRIS DISSPAIN: No. The idea is that it's -- the idea is that this is independent.

FABRICIO VAYRA: Right. But you just point out exactly --

CHRIS DISSPAIN: (off microphone.)

FABRICIO VAYRA: -- you circled back to the question that we had about --

CHRIS DISSPAIN: (off microphone.)

FABRICIO VAYRA: -- ancillary service providers and circumventing those rules.

CHRIS DISSPAIN: Yeah. Stephanie.

Sorry. I apologize, Carlton. Stephanie first, then Carlton.

STEPHANIE PERRIN: I just wanted to say that getting back to how complex that rules engine is, I mean, if you are a traveling, I don't know, Belgian citizen living in New York state, just to pick on Milton's home state, you still have data protection rights, and -- and this is going to be extremely complex to figure out where your registry is, where you're -- that's why we want a high level of harmonized data protection so that we can build that into the rules engine. "We." If you're, you know, a rabid privacy advocate such as me, you want a high-level policy that then gets reflected in the rules engine so that we don't have to --

CHRIS DISSPAIN: Exactly.

STEPHANIE PERRIN: -- tease these pieces apart, because it's a real nightmare.

CHRIS DISSPAIN: In an ideal world -- and I think I agree with you, Stephanie. In an ideal world, what you would do is you would have a policy that was at the -- at the -- at a level that was acceptable -- let's just say Ireland. Forget Europeans for a minute. European Commission. Just say Ireland.

STEPHANIE PERRIN: No, no. Anywhere but Ireland, please, Chris.

CHRIS DISSPAIN: Okay. All right.

MICHELE NEYLON: What do you have against Ireland?

CHRIS DISSPAIN: Let's say Canada. Let's say Canada, right?

And then the only question you then have is, are there any -- are there any jurisdictions that are not prepared to accept that level of privacy, which is possible, or are there any jurisdictions that insist on a greater level of privacy, which is possible.

So the clue -- the key for the policy development is to come up with your -- your benchmark and then all you have to do is move up and down either way. Carlton, you were -- you wanted to say something.

CARLTON SAMUELS: Well, I think it -- this is Carlton. You took it away, Chris, because I was saying the principles -- we have some principles and we said collection, disclosure, and transfer stayed with the latest subject. So those principles of protection stays with them.

Now, it's about the handling of the data now where you have the rules engine.

You can have an engine that -- by data subject and the rights that come with the subject. It makes those decisions. Or you could have a rules engine that implements a floor and then you go up or down, as Chris says, based on the policy that comes out of these principles.

CHRIS DISSPAIN: Okay. Thank you very much.

The line is now closed so...

You're in a virtual line. You are, of course, in the line.

MICHELE NEYLON: Does this mean you're going to give Kathy the last word?

CHRIS DISSPAIN: I had assumed that that would happen anyway, so...

Joe.

JOE WALDRON: Joe Waldron from VeriSign.

First, I would like to express my appreciation for all the hard work that went into this report. I truly do appreciate the complexity of essentially starting from a blank piece of paper and trying to address a large number of complex issues.

I would like to drill down a little bit more into the registrant's point of view. I know we've talked a little bit about that, but my ultimate question -- and I've got a couple preambles, but my ultimate question, just so you can start --- Chris, you mentioned that .CA or ccTLDs won't be impacted by this so are we creating an imbalance of, you know, significant incremental costs for gTLDs and putting it -- and putting gTLDs at a disadvantage as compared to ccTLDs?

So I think that's -- that's another factor that -- that we need to look at.

So I just kind of posed that and I think that it's important that we really look at this from the -- from the registrant's perspective in terms of complexity and also cost, and I'm just interested to know if -- if you looked at that.

I guess the other data point I wanted to also mention in the report, if I remember the -- the IBM spreadsheet correctly, the RDS component of this, they estimated, was somewhere just a little bit north of $30 million over a five-year period, so that averages out to about, what, 15 cents per name over that time period.

So that's a -- again, a cost that will likely be added on to the fees that registrants pay.

So when you start adding in the cost of running the infrastructure, the manpower at registrars, at registries, the -- you know, the RDS system, and I still believe -- this is intuitive, perhaps, or just looking at the track record of what happened with the trademark clearinghouse, a significant cost to do that validation.

So I'm just interested if you looked at what that potential impact is to the registrants.

CHRIS DISSPAIN: So Stephanie and then Carlton.

STEPHANIE PERRIN: I totally concur with your last remarks. And I would just like to throw in there I don't think you mentioned audit logs. A lot of the privacy protections and abuse protections and everything depends on those audit logs. And speaking as ex-government, that's the kind of stuff that often just falls on the floor because nobody is reading them. So it's really important that we find the money for those audit logs for the gated data.

Thank you.

CARLTON SAMUELS: Thank you, Chris. This is Carlton. I wanted to address the issue of the validation costs. We did have a lot of discussions about that. And we

heard from the UPU, which is Universal Postal Union, that they had -- they were the only ones who had very firm ideas about what validation of costs. They have so many different styles of postal systems to validate. So they're on the high-end applier.

And, as it turned out, yes, there would be some additional costs. But, compared to what you got, it was, we thought, manageable. That's the first one.

And one of the reasons we called for the risk analysis was because, if you look at all of these issues in totality about implementation with costs -- and we had IBM come and do that -- we felt that, for the policy development purposes, given the principles that we have enunciated, it would be useful to have the risk analysis executed before or in conjunction with the policy development phase. So that's our way of saying, yes, we understand that there might be cost implications. We know that the cost implications are going to come from certain areas of operation. We don't know how it's spread. But, if -- before you do put the policy in place, do a risk analysis. Thanks.

STEPHANIE PERRIN: One quick point to that, too, is, you know, I would contend some of those costs are already out there and being borne by different players in the roles and the Internet system. I mean, Michele mentioned earlier that every time he gets an inaccuracy report, that he has to do something. That's a cost. Every time I report inaccurate WHOIS information to the -- to the compliance team at ICANN, somebody's working on that, you know. And every time I have to look that up and go "Oh, this is obviously inaccurate," that's another -- you know, there's

a lot of waste and cost going on now. It may be redistributed. But I think ICANN can figure that out, too.

So --

CHRIS DISSPAIN: Speed this up so --

FAISAL SHAH: So I'm trying to understand, your point is there's going to be costs that's going to be pushed out to maybe the registrars and the registrants. And one of the things that we really thought was really important in terms of building a model around the RDS was, okay, we want to make this -- you know, have a cost recovery model, right? So within the system itself, we don't want costs being pushed down if we can actually create a system where it's making money enough so that it's recovering all those costs that it's actually incurring, right? So, to a large extent, there's a lot of different things that we point out within the document itself such as subscription fees for power users, blah, blah, blah, like a premium access piece, stuff like that that hopefully creates certain revenues that then -- you know, is --

JOE WALDRON: I would say if the $30+ million for building out the RDS and operating that over a 30-year period, I think the report recommends that be paid by ICANN.

CHRIS DISSPAIN: I thought VeriSign was going to do it for free.

JOE WALDRON: I think you read the wrong report. But that would be a significant portion of what ICANN is currently collecting for their per name registration fees today. So I think that -- again --

CHRIS DISSPAIN: Thanks, Joe.

JOE WALDRON: The costs are ultimately going to be paid by registrants. And we need to take that into account.

CHRIS DEACON: Okay. Alex, you're next.

ALEX DEACON: Alex Deacon again. On the question on the validator -- can you go to the slide, Chris, that shows the flow chart that the validator knew? That one, yes. So we've been talking about validation. And what caught my eye was this validation piece there in step 3. So this is -- this is a mandatory validation step. And is it -- is it based on kind of the existing registry or registrar agreement 2013? Or is it -- are you suggesting there's more validation that occurs there? We've talked about --

MICHELE NEYLON: Okay. I'll deal with this. Basically, we didn't ignore what was on the 2013 or the 2009 or whatever. I mean, we went well beyond that. So in the report there's comparisons between what we've proposed and what's in the current contract.

I mean, ultimately, what we were asked to do was -- you know, go back to the basics, go back to first principles, look at everything from zero. So, if the -- if, after deliberations we ended up with a situation where we reduced things or increased them or whatever, then that would be okay, as long as we were aware of what the hell we were doing.

The 2013 contract is unlike the previous contracts in that there is a process which is clear and reasonably sane with respect to making amendments to the contract should that be required.

Also, the WHOIS specifications are a specification. They're not part of the core contract. So, theoretically, at least -- I'm not ICANN staff, so I don't know how the hell that would work. In theory, not practice, it would be possible to make changes to certain elements of that without having to touch the main body of the contract.

ALEX DEACON: Can I just ask one quick question? The validators -- are all registers/registrars by definition validators also?

MICHELE NEYLON: No. What we discussed here was that validators could be third parties, could be companies that specialize in dealing with data and stuff. Or they could be lawyers. They could be registrars. They could be any

number of entities that met the requirements that -- let's just say hypothetically, there is a -- I don't know -- a certification process or a set of rules, a set of requirements, whatever the hell that works out to be. If an entity meets that and can provide that service, then they could fit into that. I mean, that's, basically, what we've said. And somebody else wants to --

CHRIS DISSPAIN: Did you want to say something first? Okay. Sorry. Cool.

>> Talking about --

>> Joe, we're talking about you.

MARGIE MILAM: You were talking about the cost. You go to page 65. It's not actually as high as he thought. It's .04 Euros is the average. So it's a lot less. Wanted to clarify that.

CHRIS DISSPAIN: Thank you. Okay.

Joe, you talk to Margie. It's easier that way.

So sorry. Hello.

MI OKUTANI: Hi, it's Mi from JPNIC. I have a question relating to the cost comparison of the synchronized model and federated model. Not in terms of the actual money. But first point I'll relate it to the earlier comment made by somebody from Canada about the cost of leakage. And I understand that -- the earlier reply that there may be high -- less risk of having data leakage if you have the aggregated model to ensure that the security will be stronger. But are there specific measures taken or something in mind that ensures this?

And the second point is I think compared to the -- I forgot the name -- the federated model, I think synchronized model adds additional layer of sharing information to a third party related to personal information. So it's not just -- within the gTLD registry, we have to share all this personal information of your registrants to a third party. So that might add additional legal issues within certain economies. Or, if there are issues related to, like, data leakage, then what would be the point of responsibilities when these kind of things happen? So what are your observations in terms of this kind of cost with the two models?

CHRIS DISSPAIN: Faisal, you want to take that? We need to be brief.

FAISAL SHAH: Yeah. Just on the synchronized model that you were talking about in terms of the security. We're talking about best practices, right? In terms of what we're going to be putting in there. You know, backups and disaster recovery plans. Everything else that we -- you know, balance loading and all the other security mechanisms that we could

put into place for a system of this type. I don't think we've gone into detail as to what specifically we're going to put in there. But, certainly --

CHRIS DISSPAIN: You wouldn't have all the data in one place anyway, would you?

FAISAL SHAH: Right.

CHRIS DISSPAIN: And you were asking about the -- did you say it was about the cost? No, it was the additional --

MI OKUTANI: -- layer of sharing personal data to an third party.

CHRIS DISSPAIN: I'm not sure that is the case. With the aggregated model -- it's -- sorry. With the federated model --

MI OKUTANI: Federated model. You don't have to share all the private information. You just refer to the information that's been queried. So, for example, you have 10 sets of data --

CHRIS DISSPAIN: Thank you. Do you want to respond to that?

ROD RASMUSSEN: Yeah. I guess it depends on how you define the sharing aspect of that, right? Are you talking about the accommodation for third party, if they're using underneath the principles for the system, to be able to have that and access the domain tools thing we were talking about earlier. Is that what you're talking about? No? Okay. Then I'm not sure what the difference at the outer edge actually is.

FABRICIO VAYRA: I mean, I think it all depends on -- this really does become kind of a nomenclature type discussion. Because, if you look at synchronized and federated, you're still talking about data that's disaggregated across multiple servers. And then, when you talk about sharing, it's really how you define sharing. It's like discussing in copyright is a RAM copy a copy? And how many RAM copies are made to display one display? The question is same thing with sharing. Did you share when you had to transport that data from the registry up to one place and display it? And is that any different than sharing when that registry sent it up to cache it somewhere? So we start to split hairs on what sharing means, I think. And I think we've been pretty educated on the fact that, from a privacy and data protection standpoint, I don't think it makes a difference, that piece, because it all falls in to a sharing type of bucket.

CHRIS DISSPAIN: We need to move on. Otherwise we're going to move out of time. I apologize.

>> Okay. I'll keep my question maybe outside of --

CHRIS DISSPAIN: You can come on Wednesday morning. We're coming back on Wednesday. I'm conscious that we need to finish with the people who have waited in line. And Wendy. And Matt.

FRED FELMAN: I'm Fred Felman, and I'm speaking as an individual registrant. I've heard a lot of people representing me as a registrant, and I just actually wanted to point out a couple things that I think are important. I have domains managed by multiple registrars. Some of them are protected by privacy services, and some of them aren't.

And recently I got from a registrar a note from someone who was telling me that my domain was about to expire. And that was protected by a privacy and proxy service, which is an indication that the registrar who that was registered with was somehow breached and that my private information was actually disclosed.

My guess is that they actually don't employ best practices data practices and disclosed my data some way in a breach.

Also, recently, from one that actually was protected by a privacy and proxy service -- actually, was not protected by a privacy and proxy service, I got a solicitation from a marketing organization, which is misusing the data, from the current system proposing that I spend $75 a year to actually get SEO help on my site.

It tells me that this WHOIS data is widely available and that the current system isn't working for me as a registrar.

Also, I would say that this data is widely available. Companies like some mentioned and some that are here actually sell this data in bulk for all kinds of purposes. And I've actually tried to negotiate some of that data to try to fill in some of the holes in our data. I will tell you that right now the system does not work and that private data is disclosed widely either accidentally or intentionally for monetary gain and not currently.

The system benefits that you're describing actually are clear to me as a registrant. And they actually harm my employer in some ways, because they actually may restrict the way that we do access data. But I still support this system because I think the current system harms registrars and causes problems. It provides gated access, which means that, as someone enters the system, they must be identified. It requires disclosure. It requires audit. These are things that are not required right now by any of the systems in practice. And, based on my personal experience and my personal data being exposed, I know that they're not using best practices. And there's rampant experience that they have as a domain naming system that data is regularly accidentally disclosed and that registrars are not informed and that other problems are having. You see that in registry problems where names have been transferred and that sort of thing.

So I challenge the people behind me in the line to actually think as a registrant and think of the abuses that are occurring right now and actually think positively about the solution.

CHRIS DISSPAIN: Thanks, Fred. Matt.

>> Hi, this is Matt Ashianti, for the record. We have a question from a remote participant. The question comes from John McCormac. The question asks, "Is the system robust enough to deal with a bad actor using multiple business fronts to gain access?

CHRIS DISSPAIN: Brief response? Fab?

>> It's supposed to be, isn't it?

FABRICIO VAYRA: Yeah. It's supposed to be. It's envisioned to. We talked about modeling data analysis and picking up variances, et cetera. I mean, the example we always used was, if someone logs in with a token and immediately starts doing 35,000 queries in five seconds, well, guess what? The system is going to be built to pick that up. If someone logs in -- and this happens today, by the way. Because we used the example of when I was at a law firm, and we loved using better WHOIS -- I think now owned by Tucows. And by noon the firm was shut off because we were all doing searches to send cease and desist letters. There was five of us. And they were tracking our IP range. And so we would have to call them every day and go, "Hey guys, it's us. Here's what we're doing." And the next day we'd get shut off again.

That was 2001. So we're talking 2014. There has to be a system that's built that picks up those types of variances. And that's what we relied on.

CHRIS DISSPAIN: Okay. Go for it.

KATHRYN KLEIMAN: Kathy Kleiman. First, Michele, not a conspiracy theory. It's just a lot to absorb.

MICHELE NEYLON: I know. I was only winding you up, for God's sake.

KATHRYN KLEIMAN: You would never do that. Can we go back to the principal purposes? I know it's been a very long session. Thank you.

MICHELE NEYLON: Compared to the working group sessions, this is nothing.

CHRIS DISSPAIN: Kathy, I am going to close this in five minutes. We do have another session on Wednesday.

KATHRYN KLEIMAN: An observation and then a question. The observation is doesn't -- aren't we working backwards here, where the use -- the purpose of the data is

defined by the use of the data? And here I'm thinking about my credit card data. I'm thinking about my healthcare data. These are collected for specific purposes.

And, if you defined it by everybody who wanted to use it in every way, the use would be a lot greater than it is now. Credit card data is used for credit purposes. Healthcare data is used for healthcare. This is used for much more than the technical purposes of domain name registration. This runs to content.

So an observation on that.

So quick question. And maybe we'll continue it on Wednesday.

But don't two principles seriously undermine the rest of the framework that you're putting together?

First principle is individual Internet use. The idea that -- as I understand it, that an individual can go in and try to identify a company that they're working with, which may be legitimate, or an organization that's using a domain name. And maybe they don't like the views of that organization. They don't like what's being said. That ability to come in and find the address and the phone number and that personal or sensitive data of any organization that you don't agree with, that's not undermined free speech, freedom of expression. Individual Internet use, undermining.

CHRIS DISSPAIN: Okay. Whoa. Whoa.

KATHRYN KLEIMAN: And then informed consent.

CHRIS DISSPAIN: I wasn't trying to stop you. I was just trying to say can somebody address the individual Internet use bubble?

MICHELE NEYLON: I'm trying to make sense of what you all said as you pushed two or three things in together.

CHRIS DISSPAIN: It means that an individual can be accredited.

KATHRYN KLEIMAN: To look for anything.

MICHELE NEYLON: No, they can't.

CHRIS DISSPAIN: So what is individual Internet use then?

ROD RASMUSSEN: That's, basically, very close to the DNS transparency is being able to do basic -- get basic information about a domain name. So that -- in that case we'd actually -- yeah. And finding the business contact and finding just basic information about when the domain was registered, all that kind of stuff. It's the public data case.

CHRIS DISSPAIN: We have explanations of what each one of these bubbles is meant to mean and, again, to become --

ROD RASMUSSEN: They don't all get access behind the gate necessarily.

CHRIS DISSPAIN: Okay. Again. On this one we all get access behind the gate. But the key here is that we can fixate on the actual words or actually say what it's -- I can't remember what it says. That's why I'm asking.

SUSAN KAWAGUCHI: Says you get the data behind the gate.

CHRIS DISSPAIN: But does it say what it's for?

SUSAN KAWAGUCHI: Sure.

CHRIS DISSPAIN: Does it say what individual Internet use --

SUSAN KAWAGUCHI: Right. So this -- and the criteria would have to be -- this is back to implementation, in my opinion.

A lot of definitions need to be put into this. But, you know, in some ways we're damned if we do and dam if we don't here. So, if the way Susan Kawaguchi would define that, if I went to a Web site and they were taking -- you know, offering a service and were willing to take my credit card, they had a shopping card on it, I really have a right to know who I'm doing business with. So, therefore, there would be some information -- maybe just the registrant name or whatever -- that I would know they are declaring they are them. Put it that way.

CHRIS DISSPAIN: Yeah, I think we -- Lisa, do you want to -- slide 40. There are 40 slides?

I'll just -- okay. Here we go. Kathy? Here we go. Individual Internet use, query scope, legal person, contact needed, business, registrant data needed. So that's what it's for.

KATHRYN KLEIMAN: Can I point out that page 27 seems to contradict that by talking about the legal postal address that appears to be public in some lists and not in other lists. So, again, an inconsistency that if developed could wind up exposing organizations for their expression and not for their credit card acceptance.

CHRIS DISSPAIN: Okay. Jean-Francois.

JEAN-FRANCOIS BARIL: So, first of all, very, very sincere. Thank you for the three hours and 15 minutes that we spent together, including two hours of full pure Q&A.

Just also keep in mind that in case you still have further questions, I'm sure you will have when you sleep over, because I think it has been very dense, we will have a session on Wednesday from 8:00 to 10:00 in the morning. Okay? And, once again, there will be two hours that we will be very happy to have everybody.

Hopefully, also, we do hope that you find this session quite interesting and quite fruitful and you find the answer of the question that you were asking because from what I have detected basically, there was very good questions, very legitimate questions. But I found out that probably most of the people get what they were asking for.

Sorry for the acceleration of our work that we have done between Singapore and now in terms of the density of our findings and the maturity of our reports. So from the preliminary report and the final report now, I think it's a huge, huge acceleration of the intensity of work that we have done here. And as such, as you pointed out, Kathy, I think it's very legitimate between what you have seen before and what you are now exposed, it is a massive amount of thing that needs to be digested. And, once again, difficult to pick only one or two topics like that. Has to be considered as one body to grasp the full intent of those recommendations. So I think this is very, very important.

As we mentioned a few times, we would be very happy to post some addendum to the report for clarification in case things have not been put in the right wording. So this is going to be orchestrated and done for all clarifications clarified for the final report.

But the bottom line lies into this room as the final question. The final question is for you to decide if the RDS that we have proposed is, in fact, a better solution and better proposal than what is currently the WHOIS system. We do hope you are fully equipped now after many digestion of this report at least to answer this question.

With that, thank you very much, everyone. And hope to see some of you on Wednesday.

[Applause]

[END OF TRANSCRIPTION]