Emily Taylor: Okay, should we get started? Thank you very much for joining our interaction with the community. We are the WHOIS Policy Review Team. And what we're going to do is just take you through a few overarching thoughts; I think you were given a copy of our discussion paper as you came into the room. I've got a few slides here, but really I'm hoping that this session will be interactive. There are mics up at the front and I'm hoping that you will use them liberally to make your comments known to us, and your views known to us.

Actually I was speaking to somebody on the way in here who said what I really want to know is what are you supposed to be doing. And so as sort of just a brief bit of context, is that when ICANN transitioned from the joint partnership agreement to the Affirmation of Commitments, which was perceived at the time to be sort of a loosening of the grip that the US Government had over ICANN. But part of the package was that ICANN would undertake three reviews.

One was on accountability and transparency and that reported at the end of last year, and then two others, one on security and stability and this one on WHOIS. Now we are the first WHOIS Review Team under the Affirmation of Commitments, but the Affirmation actually envisages that this will be an ongoing process, I think every three years.

The first thing that we had to do when we got formed, apart from doing all the normal governance stuff of decided who would do

what, is to work out our own scope. And this was something that, for those of you who attended the San Francisco interaction with the community, we were at that point consulting on our scope, our roadmap and some working definitions that we had formulated.

In brief, what we're looking at is, and this reflects the wording of the Affirmation of Commitments, we're looking at the extent to which ICANN's WHOIS policy and its implementation is effective and meets the legitimate needs of law enforcement and promotes consumer trust. So there are lots of different elements in that. We're clearly asked to look at both the policy and the implementation of that policy and to see whether it's actually getting the balance right, whether it's effective at all.

So, the next slide please. As you're all sitting there with the discussion paper and you are here at the interaction with the community, this is partly for you. The discussion paper is something – we're now six months in, we've done our preliminary work and really, at this point, there's no getting away from the fact that we have to get into the issues. Our first attempt, after this time, we're starting to get a reasonable handle on what's bugging people.

So we're trying to express those in as simple a way as possible and to frame questions about them. And the idea is that we will then take this analysis on, see whether these questions that we're putting are actually hitting the remark and sparking a response from people, and I hope that we will then deepen our analysis as

the process goes on over the next four or five months and work it up into what really will be the heart of our review.

So the next slide starts to set out the questions that you see in the discussion paper. Now, the discussion paper also gives a little bit of background. So, if I may, the background for these first two questions comes back to the way that we decided to approach our task. And we said well, first of all, we're going to inventory the policy and then we'll inventory the compliance steps, which seemed a simple enough task. And to our surprise, when we looked for an expression of the WHOIS policy we were unable to find one.

Now, there are lots of documents that refer to a WHOIS policy, certainly as many people as we've gone around the communities, a lot of people have reminded us that, of course, the registry and registrar contracts do set out WHOIS obligations. In the purest sense those are actually an implementation of the policy, they're an expression of a policy making it operational. And equally the Affirmation of Commitments itself, and indeed the GAC Principles on WHOIS also set out a statement of policy and we would like to know is this it? Is there another one that we haven't seen?

We're aware that WHOIS of course as a service, as a protocol predated the existence of ICANN by many years and was part and parcel of the set up of ICANN through the Green and White Paper. So, first of all, would anybody like to give us your views on these two questions? What measures should ICANN take to clarify its existing policy? And how should ICANN clarify the status of

these other policy type statements; one being the Affirmation of Commitments and the GAC Principles. Is that what it is? Is the WHOIS policy different? Does anybody care? Okay, so I'll go on to the next slide.

The next couple of questions are really going to be issues, the policy type issues of this balancing act, which is at the heart of WHOIS and which has led, I think – I'm acutely aware, we are all acutely aware that this issue has been hanging around ICANN and has been pretty controversial, has been viewed by many as intractable; there's a lot of weariness that we sense as we go around the different sections of the community.

But at the heart of WHOIS is a balancing act between, on the one hand, the demands to make data available, accurate, and as full as possible. And on the other hand, and certainly as somebody coming from the European Union, an expectation on the part of individuals that personal data will attract a level of protection and not be publicly available. So you have, at the outset, a conflict.

As a result of this, some registrars where there in territories where privacy laws apply, feel that the WHOIS requirements might put them into conflict with those national laws. Is that a problem? Is there anything that we can learn from implementations nationally by ccTLDs? And what do we feel about these proxy privacy services which seemed to have emerged in a policy vacuum? They have emerged as a result of a need which is being served.

And according to the figures that we've seen, about 15% to 20-ish% of all registrations use proxy or privacy to some extent, whether formally or informally. So, is there any insight that we can gain from this balancing act how others have tried to make it work? And if anybody amongst you has ideas about how to make it work…Michele?

Michele Neylon: Good afternoon, Michele from Blacknight in Ireland. This is one which I would have quite strong opinions about oddly enough. As think stand in the present, as a registrar based in Ireland, which is of course within the European Union, I'm obliged under a contract with ICANN to publish WHOIS data about my registrants. I'm also obliged by ICANN to offer bulk access to WHOIS to third parties who want it. In the same contract, I'm also obliged to protect my registrants from marketing activity. Now, maybe it's just me, but I don't really see how those three obligations can sit side by side without there being some level of conflict.

As James knows, and one of the issues we've been faced with in the registrar community is things like fake renewal notices. And the only way the fake renewal notices lands on anybody's desk is by mining of WHOIS data. And that, for me, is a huge issue. To date there is only one gTLD registry that has implemented a WHOIS policy, which I can actually sit with comfortably, and that's .tel. And for .tel to implement that policy it led to a delay in their go live, but to date I've yet to receive a single complaint related to WHOIS data for .tel. Law enforcement is happy with it.

Registrants are happy with it. Everybody else seems to be happy with it. So I cannot understand why on earth we are being forced to leave ourselves open to liability and to have to publish that private data for individuals in WHOIS, because we don't offer privacy or proxy servers at present, but I'm going to be forced to offer one and I don't particularly want to.

Emily Taylor: Thank you very much for that.

James Bladel: Don't go far, I have a question, Michele. Can you give us, maybe for the benefit of the other folks, two or three highlights of what is different about .tel that you believe makes it a better approach to WHOIS?

Michele Neylon: Sure, James. .tel is obviously heavily influenced by UK law because they're a UK company. So what they've done is they've made a very clear differentiation between a private individual and a legal person; in other words, as in a business. So, if you are a business your details go into WHOIS because under European law you have to put your details on your website anyway so why on earth would a domain be any different. However, as a private individual, you can opt-out of WHOIS completely.

So if you do a WHOIS lookup on say mneylon.tel, which would be one of my personal ones, you'll know that the sponsoring registrar

is Blacknight; you'll know when it was registered; you'll know when it expires and you'll have all the technical data that you require if you're this lady from like, this lady from [SOCAN] for some reason wants to investigate me – please don't, honestly I'm not that much of a criminal – they have access to data through a special portal that TelNIC has provided to law enforcement; and it's to law enforcement only as far as I'm aware,. I don't think they make it available to random third parties. I think there's a certain degree of validation. If you want James I can follow up…

James Bladel: No, I just, that's interesting. I'm not sure if that kind of special access would fly in the US. I've had a couple of lawyers explain it to me in a way that I sort of understand it. But I think it's also interesting just because of that .tel data is not only is the WHOIS systems containing personal data but by design the DNS itself is containing personal data. So I think that's also a unique model.

Michele Neylon: The TelNIC model for me works. I don't have an issue with it. I'm not being forced into doing something, neither am I being forced to expose extra information about my registrants and my clients. Now there is a policy-process that ICANN established for registrars if they do end up in a situation where there's a conflict between national law and ICANN policy. However, no registrar has access to that policy and process unless they are subject to a court case. So basically I have to throw myself on a sword,

metaphorically speaking, and expose myself to a massive litigation in order to access this policy and process, which to me is a bit broken. Because I cannot get that exception unless I am being sued, which is ridiculous.

Emily Taylor: Before you go…

Michele Neylon: I'm not going anywhere.

Female: Do you know how .tel came up with their definition of law enforcement; who they negotiated that with and how they ratified who is in that group?

Michele Neylon: You'd have to ask them.

Female: Oh, will do.

Michele Neylon: You'd have to ask them. I'm sorry. I know that they have it clearly defined and I know that they have clearly defined the policies. And also, conversely speaking, a company cannot opt-out of WHOIS – going back to part of the question, I'm sorry if I'm

dominating the mic, but if there's nobody else queuing up I'll just stand here for a while. I don't mind.

Emily used to work with Nominet so you know how Nominet works. It's a similar kind of process. The difference is – I'd have to do a quick look on my laptop – I don't think even the registrant name appears in WHOIS for the .tels. In most of the ccTLDs, not all of them obviously, but a lot of them, there is a clearly defined concept, a clearly defined concept of privacy for private individuals.

Now I would never defend corporations, businesses because as far as I'm concerned if they want to use a domain then they should be able to, they should say who the hell they are. Now obviously the IP lawyers may not agree on that for a whole range of different issues. But one of the key problems here, with respect to WHOIS and with respect to a lot of other ICANN policies, is we need to de-couple two things – criminal activities and intellectual property rights. We shouldn't mix the two together. And every time the two get mixed together we just end up going absolutely nowhere.

Emily Taylor: While we've got you there…

Michele Neylon: Okay, I'll stand here for a while.

Emily Taylor: Thanks. You mentioned the .uk WHOIS policy, have you got – because I understand like many registrars you'd be offering registrations across a number of cc's and gTLDs…

Michele Neylon: We're accredited across a very large number of cc's.

Emily Taylor: And thinking about ccTLDs particularly in Europe where there's a data protection regime, how common is it to see some sort of opt out?

Michele Neylon: It would be very common. Working from the west of Europe across – in .ie the only data that appears in WHOIS is the holder, the holder name, the WHOIS output is a bit different to a standard one. So in the case of a domain that will be registered to a company, so let's say domain holder Blacknight Internet Solutions Limited, and then you would have the applicant. There's two, an applicant registration type classing type think. I mean, think of it a bit like your classes for trademarks; same kind of concept.

For a private individual again, you just have the holder is Joe Soap, but no contact details for Joe Soap. There's just a nic handle, which obviously is going to be unique to the person. And if somebody needs to contact tehm for whatever reason, be that in terms of a dispute, law enforcement or whatever, they can go via the registry.

For .co.uk you've got the opt-out. And again, if they're a legal organization and they try to opt out, as part of the WHOIS review stuff that Nominet would do, they get opted back in. A lot of – I don't know how many of you have been to any of the center workshops on WHOIS; there's some fascinating stuff being done like I say with the .be registry who do spot checks on the WHOIS data.

The .eu registries do the same. So they don't, they're able to go along and kind of validate stuff and make sure that there aren't kind of weird inconsistencies like people registering as Mickey Mouse. .eu again, there's very little data available in standard WHOIS and if you want to get more data you have to go to a webpage, you have to go past a capture. And they also have taken measures to protect the email addresses. So they're rendered as a jpeg or a png or something like that so you can't scrape the data off there.

.fr has the option as well for a private individual to be opted out. And that is actually provided by the registry. And they provide an [atanom].fr.

Jim Galvin: I'm Jim Galvin. Just a quick point of clarification. You were talking about the name not appearing and only the nic handle appearing in the WHOIS output, you said if you want more information you have to go to the registry for it, not to the registrar. I just wanted to confirm that you meant registry.

Michele Neylon: You'd have to go to the registry, but not from the command line. Take for example the Write database, in the Write database or even the Sixus database, you will have a handle for an organization or a person and you can then do a WHOIS yada yada yada minus "h" WHOIS.RIPE.net; and probably the same for ARIN and the other ones. But you can't do that for the ccTLD registry. You can try but it won't work.

Jim Galvin: So I'll just take .com as a particular case because being a Fin registry, the registry wouldn't have the full contact details you would.

Michele Neylon: Yeah but most ccTLDs are thick.

Jim Galvin: Okay, so we're only talking about ccTLDs in that context. So you don't provide the same protection to the…

Michele Neylon: I don't need to because there's nothing to protect.

Jim Galvin: That's fine. I just wanted to understand the distinction.

Emily Taylor: This is brilliant.

Michele Neylon: There's nothing there. I mean if you know – I presume you've got an SSH client on your laptop – Jim and I know each other so – if you do a WHOIS look up on say Blacknight.ie for example, you're going to get back name servers, you're going to get back expiry dates, you're going to get back handles. You can't look beyond the handle.

Now, in the case of the applicant, sorry the domain holder type, if the domain holder is down as a body corporate, in other words a limited company, you can of course go to our company's house type thing and get back data there. And if somebody had, if there is the case of say a WIPO dispute, as part of the process you would go to the registry, but not via command line. You'd go contact them using more manual methods to reveal the data.

Jim Galvin: Right, you need physical access.

Emily Taylor: Thank you both for that. I think we've been looking for insights on ccTLD practices and I think one of the actions we're going to take forward as a result of that intervention is to really look into how much, how problematic the opt-out that we see in many

European ccTLDs is for law enforcement and others who want to get the information. And if anyone's got any data on that, or info to help us…Michele?

Michele Neylon: I'm sorry. I'm not taking over here but. It would be worth your while talking to the legal time in DNS.be for example. But the other thing is well, which James will be familiar with because we've both been working for the last two years on the inter-registrar transfer policy. Within the gTLD space, there's no concept of a change of control. So it's very easy, there's also a lack of clarity with respect to what constitutes a registrant, what constitutes a domain holder.

If any of you can answer the question whether what actually is, what part of the WHOIS data is sacrosanct and what part of this is fluid, I'd love to hear your answer because I don't know the answer. But if you look at the WHOIS record for a domain, is the domain registered to a John Doe or is the domain registered to John Doe who also happens to be with organization X, or is it registered to organization X, or is it tied to the email address.

Emily Taylor: Thank you very much for that. I'm going to move on now to the next slide, which I think is also about privacy/proxy and it's about this balancing act. I think we've probably covered the issues that it raises in quite some detail and it's the tension at the heart of the WHOIS debate, which is the balancing act between individual

privacy expectations or concerns and accurate and complete publicly accessible WHOIS data without restriction.

And this has been, it's not just the legal obligations, which you've heard Michele talking about, it's also the fact that the speed of access to WHOIS data is felt to be important by some stakeholders. And also, we've heard from different sections of the community, despite the comments made here, that it's also businesses who are users of privacy/proxy services and that that is felt by some communities to be legitimate because there are legitimate examples, for example before a merger, acquisition, before launch of a new product where you might want to secure the name but not reveal your plans to the world-at-large. Happy to take any comments on this or we can move on to the next issue. Please.

Michele Neylon: This is getting embarrassing. I have very mixed; personally I have very mixed views about this entire thing with relation to proxy and privacy services. However, there is one thing that I don't think has been mentioned to date and that would be with respect to whistle blowers and freedom of speech advocates. There are very legitimate reasons why somebody might wish to hide, conceal their identity. In defense of the IP holders, if I was going to launch some super cool, new, shiny product or service I wouldn't want James to know about it. I mean James and I might share a beer and all that type thing, but he's my competitor and vice versa.

If you look at some of the domainer blogs you'll see these guys, they're tracking the domain registrations. They track domain registrations of all the corporates. You'll see posts going up like "Facebook registered X number of domains last week"; "GoDaddy registered this"; "Universal Studios registered that". There has to be a balance there somewhere.

Now, I don't know what the hell it is. I'd love to have some thoughts on it. But at the same time, there is also this misconception being bandied about by certain parties, who shall remain nameless, that the mere mention of existence of proxy and privacy services is directly linked to some form of crime or bad behavior, which I personally don't think is true. If a registrant can provide their contact details in a safe and secure manner, they're going to have no reason to lie about them. However you're forcing them to provide their details publicly; they're more likely to lie about them.

Emily Taylor: Thank you very much.

James Bladel: One other thing we've heard through some of the interactions with the other constituencies was the belief, position of assertion that there is no reason why, while businesses may have some value to using privacy/proxy services, there's no reason why a commercial activity should take place on a website where the WHOIS record or the domain name is using a privacy or proxy service. And I

think that we've had some discussions where for example political or religious organizations might solicit donations via PayPal; or other situations where that could be possibly construed as a commercial activity, but they don't necessarily want to publish their name either for persecution or because it's politically untenable to identify yourself with a certain website. So I think there's, for every scenario we can cook up a counter scenario or an edge case that can give reasonable people pause to think of why these things are out there and how they can be used. Thanks.

Michele Neylon: I'll just come back one last time before I let this gentleman go ahead. With respect to your point there about collecting money for PayPal and everything else, while that's fine possibly in the US, under European law you can't do that. If you're transacting on a website you have to publish your contact details. That's not open for debate or discussion; that's the European directive is very, very clear.

Emily Taylor: Thank you Michele. Yes sir, please.

Jordan Buchanan: Hello, I'm Jordan Buchanan. Just I wanted to provide a little bit of context from previous discussions, from previous WHOIS task forces, which I participated in a bit. I think if you look, especially at the output of the most recent WHOIS task force as opposed to

your work, that task force ended up, at the task level at least, supporting the OPOC proposal, which didn't achieve consensus support at the GNSO Council level, so it's not consensus policy. But the sense of that proposal was essentially to – I think there's an assumption built into this question that is perhaps slightly wrong, which is, what is the data that's being exposed? Do we need to necessarily identify the registrant as part of the dataset what is being exposed through WHOIS?

And the approach taken in the OPOC proposal was to expose who the registrant is but not necessarily their contact information and provide contactability and a way to get in touch with someone in order to communicate with them and be able to deal wit technical or other legal issues regarding the domain name, while not necessarily knowing this is the address of that person, this is a way to get in touch with that person. So it might be a PO Box or something like that, or it might be an agent acting on their behalf, which is essentially what the proxy servers do today.

But I don't think we should necessarily assume that there's any tension between these things depending on the information that you want to publish in the WHOIS and make accurate and reliable. So if you have a set of data that's not personally identifiable but is still accurate then you've absolutely balanced these two concerns.

Emily Taylor: Thank you. Yes, Bill.

Bill Smith: I'd be interested in following up on that. So, if WHOIS isn't providing information by which I can contact someone…

Jordan Buchanan: To be clear, contactability is the goal right? It's critical to be able to contact someone; it's not necessarily critical that you know what the person's home address is in order to contact them right. There are various ways to get in touch with me as an individual. My home address isn't necessarily; it's not actually a very good way to get in touch with me. It's slow. I'm not there right now.

If you knew I was in Singapore and could send me an email that would actually be a much more reliable way of getting in touch with me right now. So I think that there's a critical goal of contactability that shouldn't be lost in this, but that's distinct from identification.

Bill Smith: Right. So, my specific sort of use case is around security related. A phishing site, a site is hacked even, okay? And malware is being distributed from a site that otherwise has useful information. In using the mechanism that OPOC was proposing, how do I quickly get in touch with that site to inform them of the fact that they are unwittingly, perhaps, distributing malware in order for them to take action for them to remove the malware or do I just then go to the registrar and say take the site down?

Jordan Buchanan: So that was the entire intent of the operational point of contact is that you – the operational point of contact is the entity that you contact in order to have that conversation. So the OPOC could be you yourself, you might be perfectly, if you're a company you're likely to actually publish information about where your IT department is or something like that in WHOIS so then you would have that contact.

If you're a private individual you might not actually have the technical savvy to actually be able to have a very useful conversation about that. You might make it your ISP or someone like that. But the point of the operational point of contact was that here is the entity that you get in touch with to deal with these operational issues.

Emily Taylor: Thank you very much.

Bill Smith: I understand that but will that operational point of contact be able to answer all of the types of questions that are going to come in. That's my question back. I gave a simple use case, there are many others; I'm just asking the question.

Jordan Buchanan: Sure. My view is that it's no different from any of the – any of the contacts today may or may not have that same failing. If you've listed your trademark attorneys as the contact and you have an

operational issue, they're unlikely to actually have the answer directly. They may have to consult other people within the company in order to get a response for you. And similarly the OPOC may be a power to deal with most of the issues that will happen, but they may sometimes need to consult with other people in order to get a good answer. I don't think that's different from any of the types of contacts that are published in the WHOIS.

Emily Taylor: Thank you. Jim and then Mark.

Jim Galvin: Jim Galvin from Afilias. I'm going to sue this opportunity, I believe what I heard what I heard them talking about in part was the priority or critical purposes of WHOIS or the system; talking about identification versus contactability.

Emily Taylor: Sorry Jim to interrupt. Would you mind just speaking a little closer to the microphone?

Jim Galvin: Yes sorry. SO I believe what I heard them talking about was the critical issues associated with WHOIS – identification versus contactability. And Bill, you brought up one point that I wanted to add, which is that there's also a timeliness characteristic that goes with both of those things, which is important. I don't know that

that's a critical purpose, but it's certainly a characteristic of many kinds of WHOIS accesses or usage that are important to keep in mind.

In any case, what I wanted to offer was a somewhat different perspective. Taking those things as the critical purpose and say well a different way to look at the WHOIS services the way in which I have been thinking about this issue now as this process has been going on, and I know that I have offered this to you in other forums Emily, it's about what community you're trying to serve.

It occurs to me that the critical issue with WHOIS – and in fact, it goes way back to the beginning when you were talking about is there a WHOIS policy and what are its origins and no one got up to the mic and wanted to speak to that question. I suspect it's because none of us know the answer to it. WHOIS policy has existed for historical or traditional reasons, it seems to me, in so far as one exists.

And I think the question we have to ask ourselves is who we're trying to serve because it's those use cases that matter and that's what drives the answer to a lot of these questions, whether you're trying to appeal to a law enforcement community or intellectual property or ordinary users or domain owners, and there's probably a couple others I'm forgetting off the top of my head. But rather than characterizing it in terms of those critical purposes I would characterize it in terms of the users of the service who you're trying to serve. Just another perspective.

Emily Taylor: Thank you very much for that. Mark.

Mark McFadden: I'm fascinated by the proxy and privacy services and how they emerged. They seem to me, in my background as an ISP, they seemed to have emerged as sort of an accident in a vacuum of the lack of another service to provide that, right. And now they actually represent, it seems they represent significant economic activity.

And what I wonder is whether or not the review team has seen numbers about what the economic impact of those proxy and privacy services are. And the reason I ask that question, is because in my mind, at a meta level, I wonder whether or not those proxy and privacy services are a permanent part of our policy landscape. I love the alliteration, by the way, and I'll take that home with me.

I think that what I worry about is that something that filled a vacuum for us and represents something that has real utility, now actually has economic weight behind it and we can't escape it. And it forms a part of our policy landscape that we can't back away from. That's what I worry about.

So I was really answering question five, I'm sorry, but what I worry about and I encourage the review team to at least try to find this data, is what the economic impact is of those proxy and

privacy services and whether or not it's so significant that we as a community will never be able to back away from it.

Emily Taylor: Thank you. Before you go, implicit in your question is an assumption that we should back away from it, is it?

Mark McFadden: Well, that would only be a personal opinion and it would be mine actually, but the other thing that I was thinking of was that as a community, as we consider our policy options, is that an option. So I know I'm answering a question with a question, I know I'm doing that, but I think that as the review team carefully looks sort of at the landscape of options to meet this tension that you've very accurately sort of described, the question that occurs to me is, are these proxy and privacy services, which are very valuable to some organizations and people, are they permanently a part of our landscape.

Emily Taylor: Thank you. James.

James Bladel: That's an interesting question. I think it's very astute to point out that they arose to fill a void, I guess, that people wanted to comply with a policy but they didn't necessarily want to expose themselves to those. So I guess the answer is whether it's an economic weight

that makes them a permanent part of the landscape or whether it's just the market appeal of those services. But I would submit that, in this is just my personal opinion, that as long as people feel that their information is both accessible and has the potential to be misused, they will want to keep those types of things at arms' length.

Mark McFadden: Very well said. And from my point of view, one of the things, I wanted to raise it up a level beyond that though and say that there might be parts of our community who are economically affected if we provided a different mechanism to meet the privacy concerns. So they might stand before you and say please don't take away our ability to provide proxy and privacy services. So that's why I was talking about the landscape more on a meta level.

James Bladel: Yeah, and I guess my point would be that they probably are a permanent part of the landscape, but they may move around from one interest to another, whether they went registry/registrar or some other third party.

Emily Taylor: Thank you. Michele.

Michele Neylon: Yeah, just going back to this operational point of contact thing from earlier. Mr. Smith was going on about possible contacting registrars. Just as a point of clarification, in many cases the registrar isn't going to be the right contact in the case of a phish. It should really go for the hosting provider. Now, they could be the same entity obviously, but it's not a given.

Bill Smith: If I could. I know, I'm aware of that, but the information that is in WHOIS is one of the things that helps us, enables us to go down and track. But if we can't deal with a phishing site in about five to six hours, there's…

Michele Neylon: Yeah but the hosting provider's going to be more responsive then the registrant in most cases.

Bill Smith: Absolutely. But if the operational point of contact isn't that entity, what are you offering through the operational point of contact, or other things, for us to deal with these issues in terms of minutes or hours? That's what I need to understand.

Michele Neylon: The problem I suppose I have is I'm completely opposed to the operational point of contact as a concept. And I don't see why you should be using WHOIS data related to the domain name when

you should actually be using data related to the IP. So you should be going to the hosting provider because, for example with ourselves, we track, we get the reports from the various security companies; we get the reports from Google and everything else and then we act on it immediately. So I mean, going to contact my registrant is probably a massive waste of time because they won't, even if they can answer you, they probably won't know how to fix the problem, whereas we can at least take it offline.

Emily Taylor: Thank you. I think we can go to the next slide, but we might be able to, or we might skip over it because I know we've certainly had one comment on this. It's really the same region we're talking about how to address concerns about proxy and privacy services and we've had some very thoughtful and interesting comments on this. Does anybody want to, before we move on to the subject of implementation, which will take the rest of the session, are there any more general comments on the policy itself and this critical balance between these competing legitimate rights and expectations? Sir.

Dave Piscitello: Dave Piscitello from ICANN. I just want to caution people to not draw too many conclusions when we only use phishing as an example of why one would want to contact a domain registrant. Other malicious activities, other criminal activities including botnets and spam and spam kind of environments are going to not

have, in particular, sites that you want to go to and contact through a hosting company. There are occasions where you really do need to get in touch with the registrant or the registrar to take action.

Emily Taylor: Thank you very much. And that is a point well made. It reminds me of the intervention that Jim made just now about who is actually the audience for this, who is the customer, if you like, although it's not a paid service in many cases. Who is it here for and what are they doing with it, what do they need to do with it?

And in our analysis so far, we've tried to think about the different uses of WHOIS and why one would want to do that. And you're quite right; it's not just for phishing sites, although that is one. It's not even for enforcement of rights always. It might simply be to just contact the registrant. Do any, Bill, did you want to come in on this?

Bill Smith: Well actually I wanted to come in on something different, which was, I've heard in a number – I want to propose a question generally out here, and that's that I've heard a number of times the comments have come up around Bulk WHOIS and the requirement to provide it, that it's used for marketing purposes…I believe all of these things.

What I'm curious about, and I don't recall seeing in any of the studies, is how frequently that service is used, number one. Is

there any traceability back to these marketing campaigns back to that data? And what was the purpose of the availability, for what purpose was this put into contracts of into the policy? Is it still required?

Male: I have no idea. But if we don't kill the echo the audience is going to leave. And so that won't help with the answers. Someone is, someone here got a copy of the local feed, the streaming and it's going into the microphones; that's what's happening.

Emily Taylor: Oh, thank you very much. Sorry, I wasn't hearing that up here.

Male: Oh you can't hear that?

James Bladel: No.

Emily Taylor: No, it sounds lovely up here. Oh how awful. Is there anything that we can do about that? Okay? How is it now?

Audience: Still echoing.

Emily Taylor: Well, how is it now? Dodgy? Well, whatever. Now, let's talk about compliance, maybe an echo helps with that.

James Bladel: I'm sorry. I think Bill had a question. I think you had a question on the table which was, what was the original purpose of that Bulk WHOIS. And it was very simple; it was put in there to ensure that back in the days of the Network Solutions monopoly, to ensure that they gave all other registrars, it was anti – it was a promotion of competition at the registrar level to ensure that everybody had equal access to registrant data so that they could facilitate transfers.

And it says in there, I believe, in that provision that as soon as ICANN believes that market power no longer exists at the registrar tier and that that monopoly has been effectively demolished, I think Network Solution is, last I checked, maybe Top Five registrar, but they're not the largest anymore. So I would say, I would submit, and a lot of registrars believe that that is an archaic provision and doesn't really belong in there anymore.

Emily Taylor: Thank you.

Michele Neylon: Going on to that question again – you asked about how many times it's been used. As far as I know, I don't think anybody's ever really used it. I know that we all, as in all the registrars, we were all contacted by an entity towards the end of last year as that entity

decided that they wanted to check our compliance with that particular provision of the RAA. So they emailed each and every single registrar from the ICANN accredited registrar list and asked us all what our policy was on Bulk WHOIS access. So we all, some of us answered them, some of us didn't. We did. We answered and told them the maximum amount and I gave them a stupid contract that they could sign if they wanted.

Emily Taylor: Thank you. Can we go on to the next slide please? The rest of the questions contained in our discussion paper relate to the second part of our scope, which is looking at the effectiveness of WHOIS implementation. And that leads naturally to looking at ICANNs compliance activities and enforcement activities. So, we start with a very general question – how effective are they and are there any aspects that you feel might not be currently enforceable, which is something that we head in different sections of the community. Does that provoke any response at all? Shall I go on to the next slide and we can – we could probably run through a number of questions and then see, but Michele, go ahead.

Michele Neylon: Yeah, sorry. I do find this embarrassing; I keep coming back up. With respect to the compliance of WHOIS, the biggest issue for registrars is where the other registrars either have dysfunctional WHOIS, nonfunctioning WHOIS or simply block WHOIS lookups. And that is a serious problem. I had one instance a few

weeks ago where the registrar in question was rate limiting the WHOIS lookups, which is perfectly reasonable. Unfortunately the rate was set at zero. So that meant that every single WHOIS lookup was immediately blocked with a totally unhelpful message saying that I had exceeded my rate, which was a bit ridiculous. And I tried this from several IP ranges in several countries and each time it was blocked.

As things stand at present there is no provision that I am aware of, for there to be any SLAs in relation to Port 43 WHOIS. There is, ICANN compliance, as far as I know, are working on doing some compliance checks, but I can see how…unless they're very, very careful they will be gamed. And even when the WHOIS service is provided, certain registrars like to play fast and loose. They will change their WHOIS output format every couple of days.

They will be compliant with the contract, yes, in that they will provide the data. However, you need to rewrite and recode your WHOIS parsing code practically weekly. I think James can speak to this as well. And that is a major pain in the rear; being blunt about it. I don't think it's, I'm not sure if ICANN compliance is positioned to actually deal with that.

Emily Taylor: Thank you. James, did you want to respond?

James Bladel: Yeah, just to emphasize that that is something that came up and I think it's in one of the upcoming points here about where one of the things we have taken away, I think, from our discussions with the different elements of the community is perhaps we need to separate the questions of accuracy and the questions of availability. And I think what you're touching on is a lot of the issues relative to availability.

Whether it's for transfer or operational purposes, but just…the anecdote is my company spends a lot of time and money and resources to produce a WHOIS system that is probably the largest in the world; when you consider that com and net are thin registries and we hold that contact data and we keep it up nearly 24/7 with absolutely zero down time. So, it is definitely not an equitable playing field when a smaller registrar just kind of let's their WHOIS go down for a weekend or more and it's that access level or that availability of the WHOIS service as distinct from the WHOIS data. So it's a good point Michele, thank you.

Emily Taylor: Jim.

Jim Galvin: So, Jim Galvin again. I'm not as embarrassed as Michele about coming up to the mic multiple times, but nonetheless. He raised an interesting point which has caused me to realize it's probably worth pointing out that in terms of the display of WHOIS information, there are different requirements in registry agreements

in the gTLDs as there are in registrar agreements. This distinction is significant.

Emily Taylor: Thank you very much. Bill.

Bill Smith: So if I'm hearing correctly, a requirement to produce the information in a standardized form would be useful.

Emily Taylor: Please go ahead.

Michele Neylon: Since this place works on transcripts nodding probably didn't help. So, just for the record, I personally would support standardization of WHOIS. There…I said it.

Emily Taylor: Thank you.

Michele Neylon: Sorry.

Bill Smith: Say this is my name and I agree.

Michele Neylon: My name is Michele and I agree. Are you happy now?

Emily Taylor: Thank you. Please go ahead.

Dave Piscitello: Dave Piscitello; I'm struggling to follow that. Not what you said, just it was humorous enough… So, talking about separating availability from accuracy, I actually think that there's a significant value in doing so. And one of the things that would be interesting to look at is the notion of repeat or persistent compliance violations in exactly what you are so concerned about, James.

If we have registrars who bring their WHOIS up, it's up for a while and it goes down and they get a notice from compliance and they bring it back up and then a couple of weeks later they do it again; and their process is basically lather, rinse, repeat over the course of a year and in a year there are 56 violations. Is there a number that we can start to think about where you sit and go look you're just gaming this? And is there an enforcement tool that the community can consider giving ICANNs compliance wherever they say you have to know satisfy a criteria or you are in violation of your contract?

Emily Taylor: Do you have an answer for your question?

Dave Piscitello: Well sure I do. I mean speaking personally, I think that people should be accountable for keeping WHOIS up in the same manner that some of the very reputable registrars keep. The whole idea is that it's up 24 by 7 as close as five or six nines as you can get is what was the spirit of, I think, the contract. So I would love to see the spirit turned into the letter of the contract.

Emily Taylor: Thank you very much. Does anybody else want to make any comments or should we move on? James.

James Bladel: Yes just quickly. That's an ongoing discussion I think among registrars as we'd like to see…and I think we did work in the latest version of the RAA, but we'd like to see expansion of this kind of graduated sanctions so that it's not just a nuclear option on the part of compliance. Maybe we went now to this; I believe there's now a system in there where there are some intermediate steps.

Maybe there could be thins idea of a minor infraction, like a little bit of downtime on WHOIS is a minor infraction, but if you pile up enough of those minor infractions well guess what, you just graduated into you're a bad registrar and you need some sanctions. But that's definitely a part of ongoing discussions that registrars want to see more of a spectrum of compliance responses.

Emily Taylor: And just before we move on, it's probably also fair to say that we've heard a similar sort of feedback, not just from the registrars but also from some of the business or IP communities saying look we don't really want someone to end up being terminated as part of this. And the support for the graduated steps of going along a line if you like. Can we go to the next slide? Well you can see the questions. I'm going to keep talking unless someone comes up to the mic.

Michele Neylon: Are you moving on to questions 10 and 11, is that it? I'm a bit confused.

Emily Taylor: If you like.

Michele Neylon: Okay, well taking question 11 for example, I think I already touched on that previously. There's an echo which is really annoying.

Emily Taylor: Is it okay now?

Michele Neylon: No.

Emily Taylor: Okay. Still bad? I think it's better if you guys talk and we listen.

Michele Neylon: I would recommend that you talk to the center with respect to the ccTLD data as they do have quite a bit. And they gave a paper presentation I think at the center GA last October, which was interesting. Then the DNSB guys, .eu do a certain amount and .co.uk, as you know used to work for them, do the same. Don't talk to .ie because theirs is quite broken. .es I'd keep away from. I'll shut up now so I don't cause trouble.

Emily Taylor: Thank you. That's very helpful. Any more on these about what ICANN should do to ensure its commitments are effectively enforced? Does it need any additional contractual powers to help it do an effective job? This is horrible. It's really awful. Is this better?

Male: How about this one? Oh very nice.

Emily Taylor: Alice could you move on to question 11 because I think we're – Michele answered question 10. No, it was question 11.

Bob Hutchinson: I was curious, there seems to be a wide range of accuracy of WHOIS data itself from the registrants information. I was wondering if some of the registrars could speak to what they do to ensure accuracy of the data in today's world and if they believe that there's any way reasonably to improve the accuracy that could be institutionalized. I've been on a couple of the WHOIS teams and things have been tossed around like verifying the addresses through address verification databases and things like that; known good addresses. There are identity verification services, but there's a debate as to whether that amount of money for registrars would not be cost recoverable for them. So I'd like a registrar who may have looked at this to address that.

James Bladel: I guess that falls to me.

Michele Neylon: I'll back you up James, don't worry.

James Bladel: Okay. So this is a sensitive topic for registrars because we believe, I think and I'm paraphrasing here because I'm the only one up here, but that this is a difficult and challenging system that looks very simple on the surface. Just go and verify this data on the inbound and you won't have all these accuracy problems. The problem is that it turns out, when you start to unravel this, it's very, very difficult, very, very slow; it's not real time and it's very, very

expensive. In some cases the wholesale rate of verifying…because I can't even…is this any better? Okay, we're going to pass this around the table. Thank you Bill, great idea.

So it boils down to where's that threshold of what we call, in contract language, commercially practical verification. And you know, it is a sensitive issue. I would say that perhaps one of the balances is we take a look at what we can do in terms of being responsive when we do detect invalid WHOIS and we have a system for that, the WHOIS Data Problem Reporting System. And we can maybe enforce what registrars are doing to respond to claims that there is an invalid or an inaccurate record.

But you know, I think that when you start talking about things like that you open up a lot of interesting questions, not the least of which is how do I now effectively compete outside of my own national boundaries, which is fine for me because I've got the US and Canada; Michele may not be so happy with that, being stuck with Ireland for example. So it opens up a lot of interesting questions in the implementation that I think registrars would like to make sure that we're fully appreciating those and we're not just saying here verify this.

Emily Taylor: Thank you. Please go ahead.

Jordan Buchanan: Hey. Jordan Buchanan again. Just as a note comparing the current policy framework versus what you might be talking about. The current policy and the current contracts don't require registrars to verify accuracy upfront. They require registrars to be responsive to claims of inaccuracy after the fact and they require registrants to provide accurate information at the time of registration. But there's not currently a requirement for registrars to do any verification at all of accuracy at the time of registration.

Michele Neylon: One of the things – we had a meeting between the registrars and law enforcement yesterday – I think it was the law enforcement…or was it the GAC? I think we had both, no it was the GAC actually. And one of the key problems that we identified is what constitutes a correct address? What format is the correct format for an address in a particular country? The UK has a standardized post coded system. The US has its zip code system. I come from a country where there is no standardized format and a company as large as Google – hi Google – they can't even validate the addresses properly. So what hope to I have?

One of my staff, for example, comes from County Cary, which is down at the Southwest of Ireland. For those of you who haven't been there it's nice and rugged and rough and what have you. And because the towns and town lands are so small, it's possible to put first name, last name, town, Ireland. And of course the post will arrive, there's no issue. It's not even much of a debate. I mean even for me, I've got an odd surname and I've got an even odder

first name and I do get post which would be addressed to some bastardized version of my first name followed by some bastardized version of my surname, Ireland. And this is quite normal. So how on earth do you expect me to validate an address in Kazakhstan?

James Bladel: That's a good story. And for all the, if there are other Americans in the audience that are thinking that that sounds very quaint, I grew up in Iowa. My wife's address most of her life was Rural Route One. That's it. That's a valid postal address. It also opens up an interesting question of how do we respond to things like post office boxes, or for the military, APOs and FPOs military post office boxes. Are we saying essentially that because we could not validate these, those folks can't participate on the internet?

Bob Hutchinson: Well with the risk of bumming out Bill Smith entirely, the team that I've been working on is the internationalization of WHOIS data. And when you start to look at this through the lens of scripts and how the WHOIS data would get represented in Uzbekistan, and how the number of languages even within that country could be represented. And what requirement you are placing upon the registrant to register, for example, in ASCII characters, for example. Okay? This becomes a very huge area that I don't see being addressed on your slide ware. And we've struggled with it as a team quite a bit. So it's another item you should be paying some attention to.

Emily Taylor: Okay. Bill.

Bill Smith: So this is Bill Smith for the transcript; if we have one. You might be surprised that I'm actually incredibly supportive of internationalized domain names; at least personally. I won't pretend to speak for my company at this point. But I've actually supported internationalization for over 15 years; both individually and trough team members that I supported when I was at Sun Microsystems. So I think it's critically important.

Bob Hutchinson: I didn't mean to imply…

Bill Smith: No, no I know. I just want you to know actually…

Bob Hutchinson: I'm talking about the registry data part and not the…

Bill Smith: No, no even with that. I think PayPal, eBay, all of us, we need to deal with that issue. And requiring people to out information in that's seven bit ASCII clean is just insanity. In the world where there's so many scripts, different languages; we just have to deal with it. And the longer we wait the worse it gets.

Emily Taylor: Thank you for mentioning that. There are two contexts in which this is highly relevant. One is in relation to existing WHOIS policy. The recent data accuracy study highlighted one of the significant causes for seemingly inaccurate WHOIS data at the moment is in problems with translating or transliterating from other scripts into ASCII. So it's clearly caused internationalization of WHOIS data, is causing – I don't like to use the word problem in this context, but it is seemingly a cause of inaccuracy although it is in fact something that gets lost in translation as it were.

Our task it to look at existing WHOIS policy. And so of course, just as for new gTLDs, we're not looking at what might be. We're trying to look at the landscape as it is, but thank you for raising that point.

Dave Piscitello: Dave Piscitello; ICANN. One of the things that I ask you to consider is if you look at accuracy and you try to think of the entirety of the registration data, all the elements, it is an imposing amount of information to try to verify. On the other hand, at least to my knowledge, most of the registrars rely extensively on the email address.

And if there were a way to improve the accuracy of email address to have a high level of confidence that the email address actually reaches a point of contact, for example a click back, which is the way that many web portals where you have to have a subscription

verify that there is actually a human being submitting a name and then perhaps a capture or something else like that. There are ways that you can actually improve that particular piece of information. And since that is the vehicle that many registrars use to provide notifications, to request renewals, and most importantly to request someone go annually and update their WHOIS, it seems that at least a nice baby step would be let's try to get a WHOIS that has all, a very high degree of accuracy with electronic mail addresses.

Emily Taylor: Thank you very much. Mark.

Mark McLaughlin: I just wanted to respond to my friend Dave here; because as a registrant, my experience is that my registrar contacts me by email I think once every six months or something like that. And I know I have people that are in my office building who get those same mails for their domains. And since they come regularly, and have the same predefined format, they're simply treated as Spam. And so the very tool that we have in place now for actually validating those email addresses probably is, at least for…

[background conversation]

Mark McLaughlin: I'm just responding my experience as a registrant. I hear ya.

Emily Taylor: Okay, we'll go on to the next slide if we may. Oh sorry, yes.

Female: So actually that's a good point and I know that I frequently set up different accounts at different registrars when we're transferring domains, recovering them. And frequently to set up a new account, I can't complete the account information until I've received an email and responded. So a lot of registrars are already doing that for the account information so why can't we implement that for the WHOIS information? I agree with that completely.

Emily Taylor: Sarmad.

Sarmad Hussain: I wanted to take a step back and comment on the internationalization of registration data just as one comment in the context of data accuracy. That is that if we actually allow internationalization of WHOIS data that is actually going to improve WHOIS accuracy in way because it will obviously get rid of some of the transliteration of translation errors which are in the data. Obviously that will also have an impact on accessibility of that data, but I just wanted to bring that comment in; that accuracy is actually going to improve through the internationalized data.

Emily Taylor: Thank you. Michele.

Michele Neylon: Yeah, actually speaking to the thing about email. One of the problems with that is you're assuming that the registrant has email; not all of them do.

Emily Taylor: Thank you.

Michele Neylon: I can't hear you. That's not true. You can register, there's nothing to stop you from registering a domain name without having an active email address at the time of registration. Because I could give you a paper form to fill out, depending on my business model, and you could post me back in a check for the payment and for the registration. It's how certain business models work.

Female: That's how they used to work.

Michele Neylon: But it still works in some areas. I mean we are involved with a very large campaign involving Google in Ireland, which is to get a lot of these businesses online. And we discover that a relatively high proportion of them don't have email. For this audience it's like oh my god, somebody who doesn't have email. How could

they possibly survive? Well they've got telephones. They still use typewriters. The world still goes around without email.

James Bladel: Can I just touch on one thing I think was very important that Dr. Sarmad and the gentleman here – I'm sorry Bob?

Bob Hutchinson: Hutchinson.

James Bladel: Hutchinson, thank you. Now if we start to couple this internationalized contact data information with a prescreening requirement, let's say for example. Now we've got a really interesting issue where we were saying for example, that registrars are now confined to competing with their own country; now they're confined to competing in their own language as well as in their own country; or in languages that they understand or can know.

So I think we have to be careful when we start talking about in our desire to achieve higher accuracy that we don't put up, what I'm going to probably misuse a term of art here, but barriers to trade and creating silos where certain registrars can't actively engage registrants outside of a certain area. So there will be artificial picket fences going up around certain markets based on geography or language or what kind of address system they use. Thanks.

Emily Taylor: Thank you. These questions here are talking about accuracy of WHOIS data and also whether any lessons can be learned for ccTLDs about data accuracy. One of the comments I think made earlier was about, and several people have mentioned this, about the range of what we mean by accurate from super, super amazing and fully accurate to something that's good enough to contact even if it's only be the email. So…Olof?

Olof Nordling: Just a quick message we got from the technical staff that the feedback problem should be fixed so you should be able to use your table microphones.

Emily Taylor: Thank you. Good. So, any comments on data accuracy, and ccTLDs in particular?

Male: Actually I just had a quick follow-up question, actually a comment first with respect to your email accuracy and actually in response to yours. I actually do believe that if we can assure email accuracy in whatever way would do it, it would improve the WHOIS data significantly. And I think the people who don't actually have an email address who actually do have a domain name is probably, in the grand scheme of things, fairly limited; a small fraction of the overall population of domain name holders.

And my other point was actually with respect to your address, since I've got you up there right now, with respect to your address points in Ireland where I can say I want to send it to a bastardized version of your last and first name and just say Ireland, but there is probably still some kind of standardized postal system somewhere in place…

Michele Neylon: Not when it comes to addresses, no. We don't have post codes. The only part of Ireland that currently has post codes is Dublin.

Male: But I'm not saying that you necessarily have a post code, but you at least have probably the town is actually a legitimate or the municipality which has been actually recognized by…I mean I don't know in Ireland at all so I'm just asking.

Michele Neylon: Not really, that's the problem. Because depending on which part of the country you're in you could be referring to a town, a town land, a city. Now the order in which things appear would be standardized in that you'd have name, address, in that order. And we wouldn't be capitalizing surnames of anything like that, but actual the standard thing, how many characters long, how many lines do you need – maybe the post office has some system in place, but we don't have a post code system. Wish we did but we don't.

Male: Well anyway, I just wanted to understand the problem overall because I wasn't quite clear on what…

Michele Neylon: Well the problem I suppose is if as a registrar you are working on the basis of pretty much automating pretty much everything wherever you can so that everything happens in close to real time. So, if we are being asked to validate the address data at the point of registration or at the point of signup, which may or may not be the same thing, in order for us to do that in an automated fashion, we would need to know what a valid set of data looks like.

So this is the problem because in the UK I know that I can check against the post code, I might not be able to check against everything else, but at least the post code does follow a standardized, what is it, six characters long. In the US, they have the zip code. And in other countries, like I say for example, France it's the [CEDEX, the department]; all that kind of thing. There are standardized things. But that doesn't work for all.

And then to James's point about PO Boxes, I think it's the Caymans where everybody has a PO Box; there are no streets or something. I remember this has come up in other discussions. So a PO Box is the standard way of sending mail in some places.

Emily Taylor: Thank you. Shall we just move on to the next slide if there's…sorry. Oh do you want this one? We can give you this mic now and you can just stroll around with it.

Dave Piscitello: This is Dave Piscitello. One more comment and I will relent on this for the day or at least the hour. FedEx solves this problem. International postal, I mean the uniform postal union, or whatever it is, has conventions and people ship packages to little villages in Ireland and to Samoa and to God knows where.

So I think that part of what we encountered when we were looking at addresses in the International Registration Data Working Group was there are conventions and I think maybe this community needs to have a little bit more of a dialogue with those entities that are actually solving this problem on a daily day because they're making millions of dollars doing it.

James Bladel: FedEx does do a pretty good job; UPS as well and other systems, but they do not have 100% coverage.

Dave Piscitello: We get to FedEx level of quality and I'll be very happy.

James Bladel: Yeah. I know that when we get into a lot of situations like over in the US where people will compare the postal service to FedEx.

And well like the postal service doesn't get to choose who it serves and who it doesn't serve, FedEx does.

Emily Taylor: Thank you. This is the last slide you'll be relieved to hear. And it's really talking about what's the impact. So if nobody bothers to enforce or comply with WHOIS obligations, so what? What are the consequences? And also, what are the difficulties and the costs and the barriers to compliance? So it's trying to look at it from both ways; how much does it cost and why would it be difficult to comply on the one hand, and on the other hand, so what if you don't. What is the impact for noncompliance for users, for registrars, for ICANN? Jim.

Jim Galvin: Jim Galvin again and I'll just use this as where I wanted to bring up my point from earlier, which is the consequences of not having it just depends on the user community you're trying to serve. I mean that's really the simple answer. And then you have to explore each of those use cases to really expand on that question.

Michele Neylon: It's Michele. That's not actually entirely true. Because under the, if WHOIS policy is mandated by your contract and you're found to be noncompliant then it can have a direct impact on your business. So I kind of disagree with you.

Emily Taylor: Any more thoughts on this? Dave.

Dave Piscitello: You actually mentioned something – well I guess it's on 12 you have "barriers, cost" and then you have "otherwise". I think one thing that would be very interesting for the community to consider is, understanding the burden in a more quantifiable manner and understanding how the burden can be either distributed or relieved off the people who currently feel that they burden is too great.

And so in other environments if you go to, like an Obama cyber security summit and people are talking about ISPs having to do filtering or this is an extensive logging of every single transaction and providing it to the US Government – that's a significant burden for some ISPs. And one of the things that you'll hear being entertained is well is there subsidy. Is there a way to distribute the cost? Is it inappropriate entirely to not shed some of the costs on the consumer?

And I think we haven't had enough of those dialogues here and in some cases that tends to polarize the community into the people who are going to have to do it and pay for it with no actual revenue model, and the people who feel it's actually necessary for them to do so.

Emily Taylor: Thank you very much. Mark.

Mark McLaughlin: Yeah, Mark McLaughlin and I agree with Dave completely on that and that sort of frames my answer for number 13. In that so often when we talk about the consequences of noncompliance, the consequences are anecdotal. We tell stories about what the consequences are but we don't really measure them, we don't identify and provide metrics that we can actually use to discover whether we're doing better.

And those metrics are hard I think, they're hard to come by, but that's got to be one of the answers to number 13 is rather than a continued reliance on anecdotal evidence on a use case by use case basis, do the work that's needed to be done to identify metrics so we can tell whether or not we're doing better.

Emily Taylor: Okay. I'm going to wrap up now. Bob, would you like to make one last comment before we go.

Bob Hutchinson: One last comment. One thing you might consider, similar to the Anti-Phishing Working Group or others that are monitoring the health of things, there doesn't seem to be a place where people who have had compliance or failure issues with WHOIS can log the complaints easily. I don't know where to go to do that myself. Pardon?

Emily Taylor: Well thank you very much ladies and gentlemen; both for sticking with the echo and also sticking with the dialogue over the last hour and a half. And also, I think having an interesting and cordial discussion and difference of views on this subject, which I think is a success in itself. We've heard lots and lots of very interesting and thoughtful ideas about how to direct our own work and also your ideas about how things can be improved.

Yeah, I threw that out straightaway, I just threw it out straight away as soon as I saw that picture. Anyway, some of the ideas that have come up – we've heard about the policy in .tel, a number of different ccTLD implementations of WHOIS that you've advised us to look at. To ask ourselves about the critical purposes of WHOIS, whether it's contactability, timeliness of contactability, and what the priority is for identification. But also the key different buckets, if you like, of priorities – availability of the service, the importance of maintaining that, the cost of maintaining that, but also, the accuracy of the data and several calls for a standardized format of capturing and displaying the data.

We were advised to look carefully at the impact of internationalization, both of WHOIS data and of gTLDs themselves. The importance of use cases, thinking about who we're serving; and the importance and difficulty of achieving metrics on both the economic size of things like proxy/privacy, but also the difficulty of finding metrics to evaluate the harm caused by lack of compliance. This has been a very, very rich discussion. Thank you all for your input. And thank you for your continuing

following of the review team. I'll look forward to receiving comments from you in the consultation process and our next update in Dakar. Thank you.

[End of Transcript]