ICANN72 | Virtual Annual General Meeting - Joint Meeting: ICANN Board and SSAC
Tuesday, October 26, 2021 - 16:30 to 17:30 PDT

AARON JIMENEZ: This session will now begin. Please start the recording.

[Recording in progress]

AARON JIMENEZ: Hello. My name is Aaron Jimenez. Welcome to the joint session with the ICANN Board and the Security and Stability Advisory Committee.

Please note that this session is being recorded and follows the ICANN expected standards of before.

Interpretation for this session will include six U.N. languages: Arabic, Chinese, French, Russian, Spanish, and English. Click on the interpretation icon in Zoom and select the language you will listen to during the session. For our panelists: Please state your name for the record and the language you will speak, if speaking a language other than English.

Before speaking, be sure you have selected the language you will speak from the interpretation menu. Also please be sure to mute

all audible notifications and speak clearly and slowly for the interpreters.

This discussion is between the ICANN board and the SSAC. Therefore, we will not be taking questions from the audience. However, all participants may make comments in the chat. Please use the dropdown menu in the chat pod and select "respond to all panelists and attendees." This will allow everyone to view your comment.

To view the real-time transcription, click on the "closed caption" button in the Zoom tool bar.

With that, I will hand it over to ICANN board chair, Maarten Botterman.

MAARTEN BOTTERMAN: Okay. And in the background, that was Leon's dog, not mine.

He hears me.

So sorry for that. But really welcome everybody. Welcome, Rod. Welcome, SSAC members, for this session with the board. Your work is at the core of what we do and the core of our mission, the security and stability of the unique addressing system that we offer to the Internet.

And really look forward to be able to have an open discussion about some of your recent reports and about our interaction and how to do this best.

So the best person to facilitate this is the woman that you sent to us to liaise with your work, Merike Kaeo.

Merike, would you be willing to take this away?

MERIKE KAEO: Absolutely. Thank you, Maarten.

And I want to welcome my board colleagues and my SSAC colleagues to this session. And, hopefully, we'll have a very full hour of good discussions.

And I also want to welcome all of -- everybody in the audience who's listening in.

So next slide, please.

For the next hour, our agenda is as follows: First of all, the SSAC will discuss and bring forth some of the recent publications, so specifically, SAC117, which is a report on the root service early warning systems; SAC118, which is the SSAC comments on the initial report of the expedited policy development process, EPDP,

on the temporary specifications for gTLD Registration Data Team. And boy -- Phase 2A -- and that was a mouthful.

And then also the SAC114 update, which was the SSAC comments on the GNSO new gTLD Subsequent Procedures Draft Final Report.

And so once we go over each one of these publications, I will open it up for discussion. So if the board colleagues have any kind of questions that the SSAC can answer, I would very much welcome that.

And then the second part of the agenda is for the SSAC to provide input on the board questions, which the first one was, how could ICANN efficiently identify and work more closely with the governments globally, as well as educate, train, and interact when it comes to geopolitical issues relating to ICANN's mission?

And the second question, are there any improvements to the current process the board uses to address advice that you would like to suggest?

So next slide, please.

So at this point, I'd like to welcome Geoff Huston to talk about SAC117.

GEOFF HUSTON: Thank you for that.

And good morning, good evening, good whatever, all.

I had the pleasure of chairing the SSAC working party that looked at this particular topic.

It was prompted by a publication from the office of the CTO, going under OCTO 15. And it's looking at the concept that we accept as a common truth that the root zone cannot grow to infinite numbers. When we try and sort of think about a trillion labels, or even a billion labels in a root zone, we really have no idea how it could possibly be supported by not only current technology, but, you know, potential future technologies that we could envisage.

So somewhere out there in the future is a point where the root system could not carry on as we currently know it.

The discussion has been, if we know that there is a discontinuity at some point, can we forecast when we are approaching that discontinuity? Is there a point where we could forecast some kind of, let's say, imminent, but I suppose the correct adjective is predictive, predictable point, where further changes to the root zone, either in population or behavioral character, would cause irrevocable changes in the nature of the DNS such that it would

sustain damage and cease to function, and irrevocable such that we could not retrieve the situation unless we eliminated some aspects of those changes.

Now, in studying this question, particularly in a lot more detail than was in the OCTO report, we tried to look at exactly what was going on here. And although it might seem to be a simple system, the DNS behaves a lot like chess: bounded systems, simple moves, extraordinarily complex behaviors. And the root zone is certainly at the heart of that level of complexity.

And I use the word "complexity" rather than "complicated," because in some ways, in a complex system, we have to admit the possibility of emergent behaviors. And that's certainly true in the root system and in the DNS at large.

And the result of that is, it is extremely challenging to understand how we could instrument the DNS and the root zone in particular to actually forecast imminent failure, to forecast that point at which further changes of whatever we were doing at the time would cause the system to effectively collapse.

Now, this is, I suppose, a clarification to earlier points of advice and commentary that SSAC has made, where SSAC has certainly noted and supported this concept of a so-called early warning system, that we should build such a system to sort of give us an

understanding of when we might be close to approaching some point of change or, at worst, failure of the system.

Now, in so saying that we do not understand how such a system could be built at this point and don't think that it is feasible to build at this point, we are not -- and let me emphasize "not" -- criticizing the efforts to instrument the root system. The data that is being gathered and the further data that RSSAC in particular is envisaging collecting about the behavior of the root system is of extraordinary benefit. And while it doesn't necessarily inform us as to when we might be close to collapse or some other kind of irrevocable change, it does inform our efforts, both technically and in policy terms, as the nature of the root service and the DNS at large.

And so we are very much in support of further efforts to undertake measurement programs and to instrument the DNS root system and the ways in which the root system is being used and queried. And this is, on the whole, beneficial.

But do not confuse this -- is the point of this particular advisory -- do not confuse this with effectively a prediction that all will continue to be well or a prediction that there is a problem looming. The fact that we can measure what we are doing today and the fact that I think we understand, or we collectively think we understand the way the root works does not necessarily mean

that if we were to change the parameters of the root system by population, by behavior, by query protocol, it does not mean that today's measurements would extrapolate into the future and give you the same outcomes. We are unable, in our estimation, to instrument such early warning systems at a technical level.

I think it's, you know, the best explanation I can give you, Merike.

And with that, I'll hand it back to you. Thank you.

MERIKE KAEO: Thank you very much for that detailed, and I think very thorough explanation of SAC117.

I want to invite any of my board colleagues to ask any questions that they have. But I do see that David Olive's hand is raised.

So, David?

Is that correct?

Okay, Maarten, I saw that your hand was up. Did you have a question?

MAARTEN BOTTERMAN: Yeah, for sure.

I appreciate what you say, Geoff. And we were first in the guessing game, with various limit. I think to move from the guessing game to a measuring game makes a lot of sense, something we need to do anyway. We need to know when we see peaks that threaten the root server operating at any time, anyway. So I appreciate that.

So taking into account and assuming that the next round would be in the thousands, like the last round, can we safely assume that that would be safe?

GEOFF HUSTON: That's a leading question which I find difficult to answer.

There is always this issue with noting that the inevitable outcome is unsustainable. And as I said in the introduction, if we talk about a root zone that contains billions or trillions of entries, we have no idea how to do that.

And the issue comes every step where we talk about a hundred or a thousand. It is difficult before the step is taken to perceive what pressures or eventualities might occur even in that small incremental step that would change the behavior.

What we have noticed with many computing systems -- and multiuser computers are a typical example -- is that catastrophe

occurs as a need, that the system is perfectly capable of absorbing incremental pressures until it's not. And when it's not, the failure is complete rather than incremental. It is catastrophic. That it's not the plus one user. It's by the time you get to a million, a trillion, whatever the number is, the system completely collapses. And the ability to predict in advance when that next increment occurs is something that the system doesn't admit to.

So the signs say all is good. But I could use an ancient Roman technique of observing the entrails of something handy to make that prediction just as readily as I could look at the current technical data to make that prediction. We just don't have enough data about the complexity here. You know, this is a system that is complex, and we cannot offer you that level of assurance that everything will be fine at each step along a journey where we understand ultimately it won't scale. But we really don't understand the point and the reason why that won't.

So I'm very hesitant to offer you any degree of assurance here, Maarten, that any incremental step is safer than any other. All we can say is so far, it's worked. And that's a true statement.

MAARTEN BOTTERMAN: Yeah. So even for a couple of thousand, you would be still uncomfortable making that statement? And I'm not negating that we shouldn't measure. It's just that we have some experience by

adding those couple of thou- -- 1500. And we've seen the effect of that; right?

GEOFF HUSTON: There is a broader architectural point that we probably will be studying further.

The DNS works because it's a hierarchy. And that hierarchy gives us incredible caching properties. If we didn't have that degree of concentration of query and query diversity at the root, the DNS would never answer your queries.

If everything had to be a live search through every authoritative name server all of the time and caching didn't work, the DNS would not behave in a way that is usable by people. That's easy.

Flattening the namespace and removing that hierarchy decreases the efficiency of caching at high-query volume locations.

And so as we further flatten the namespace, we pay a penalty in DNS performance. Now, the observation that we have today is that the shift from 4 to 6 to 200 to a few thousand hasn't appreciably changed the behavior of the DNS, and that's perfectly true.

What we don't understand is that incremental performance penalty against incremental changes, and that's an interesting topic of future study about this whole issue of catchability and the advantage of hierarchies in this name system to give us performance, which is what we all strive for, versus the issues of the namespace itself.

Flattening it solves other problems but creates some as well. So that's certainly a topic for future study.

MERIKE KAEO: Thank you for that. I am looking at the time.

MAARTEN BOTTERMAN: Sorry.

GEOFF HUSTON: I'm sorry. Long answer.

MAARTEN BOTTERMAN: No, no, no, no. Just the same is true for DNSSEC. I get it. Appreciate it. So thank you very much for your answers.

Please, Merike.

MERIKE KAEO: Sorry, Maarten. I'm just looking that we're spending almost 20 hours on one topic -- I mean, 20 minutes on one topic.

I do want to have the discussion and want to make sure that everything is clear from both sides.

I do see one hand from Patricio. And so please do ask your question as well.

PATRICIO POBLETE: Just quickly, first of all, you get to a billion, it won't happen all at once but one step at a time. And I think in that situation, what you want to have is the widest possible diversity in hardware and software for the root servers so one of them could serve as the canary in the mine and tell you what that doom is impending before all the rest collapses.

GEOFF HUSTON: Can I quickly answer that, Merike? It does involve, I suppose, a salient topic here.

So far we have provided competition and diversity in the characters, the words that we use in the root zone. At some point, this industry might well move into competition in behaviors and actually giving a diverse DNS experience by having different labels invoke different behaviors in the DNS itself.

If that happens, we will be entering a space where we have no practical experience. We have so far used a very uniform DNS where the behavior of the system's independent of the labels being queried.

We've had some slight experimentation with IDNs where work is done at the edge and then conventional resolution occurs in the middle. And that's certainly posed its problems.

If we move to more behavioral diversity and introduce computation as well as serving of names, we will create an extremely different DNS whose dynamic behaviors at this point are entirely unpredictable, and not just unpredictable for the changes but unpredictable for the change as a whole. Changes imperil the entire system, not just the bits you changed. And that's sort of the caveat that this is an area to proceed with due caution as being the most appropriate response. Thank you.

MERIKE KAEO: Thank you for that, Geoff.

And for those that may not see the chat, John Crain also added some context that ICANN is, of course, very supportive of both the RSSAC002 and 047 measurement efforts and that there is some prototyping that is going on for others to use.

And as OCTO troubleshoots and gains experience with this system, I think they will consider the best way to publish the measurements. So just wanted to add that bit of context, too.

All right. Thank you very much, Geoff and for my Board colleagues for a very informative discussion.

Let's move on to the next topic, which I believe is SAC118.

So Steve Crocker, take it away.

STEVE CROCKER: Hello, everybody. Pleasure to be back with you all again, even virtually. SAC118 is a report that came out of our involvement in the GNSO expedited policy development process Phase 2(a) which, as you understand, followed Phase 2 and followed Phase 1. So it begs the question of exactly what "expedited" means in this context.

Phase 2(a) focused on two specific questions, whether there should be a way of distinguishing legal persons versus natural persons, that is businesses versus humans, in the registration process; and if so, whether they -- that information should be used to treat the registrations differently.

And the other question had to do with pseudonymized email addresses, which I want to speak to quite separately.

In both cases, as part of our involvement -- and I want to mention that Tara Whalen and I were the SSAC representatives and participants in the working group. And Tara has been involved in this process far, far longer than I had been. And I want to make sure it's understood that even though I'm doing the talking at the moment that quite a bit of the heavy lifting was on her part.

In both cases, for both of these questions, although we participated very actively in the working group and contributed our perceptions and comments and so forth within the confines of the policy development process, which means that there's a charter and a particular set of objectives, that we also came away with some strong feelings that there was something deeper that was broken basically.

So I want to -- and on the basis of that, in addition to all of our contributions which were within the process, we wanted to step outside of the process and speak from an SSAC perspective to you, the Board, and to the community in general and make a couple of observations.

So with respect to the legal versus natural persons, it became evident that there's a huge amount of energy being put into

whether or not that data should be collected, how it should be used, and how -- how much one could depend upon it, what the risks were of making the wrong decision, what happens if a natural person was treated as if they were a legal person and vice versa, all related to the GDPR and its rules about privacy.

And the emphasis on trying to squeeze out the maximum amount of access to public data -- let me phrase that slightly different. The emphasis was on -- by some parties including some of our SSAC colleagues was how to minimize the amount of data that was considered nonpublic and, therefore, maximize the amount of data that was available publicly. And participating in all of that and listening and trying to understand what was actually going on, it became evident that a major source of concern that was biasing and driving a lot of the discussions was an implicit lack of credibility that access to the nonpublic data would be coming along in any kind of useful, effective, appropriate way.

That's a serious issue. The context of the whole EPDP process was, at least large fractions of it, are on identifying what had to be made public and what had to be protected as if -- well, with the understanding that the rest of the system would somehow come into existence and be defined. And, yet there is no evidence that such a thing is actually going to happen.

So we made a point of writing this report as an SSAC report and reporting to you. And there will be, I think, other things that will happen along the way which would say, "This is not good enough."

If I remember the order of the slides, some of this is on the next slide, I think. Yeah.

So here's five attributes that should exist if there were going to be an effective way of getting access to the nonpublic data for appropriate purposes by appropriate parties under appropriate controls and review process.

"Timely" in this context means that not that the responses come quickly -- that's a separate issue -- but that the system comes into existence in some reasonable amount of time.

"Reliable" means that it operates in a predictable way and consistent way so that users know what to expect and can depend upon it.

And "useful" and "efficient" have to do with it actually being fit for purpose and easily accessed is -- that the costs and bureaucratic hurdles and so forth for getting access to it are within some reasonable balance.

So this is a -- you can view this as provocative if you want, but it's intended to be a challenge to whether or not we have any handle on whether or not such a system is going to come into existence and, if so, whether its attributes would be meaningful and appropriate for everybody.

And as I say, all of this is in recognition that the reason why there was an extraordinary amount of back and forth and not very satisfactory discussion about the fine-grained details of distinguishing legal versus natural persons was really being driven, in our view, by a belief that those distinctions would matter greatly, even to the people who should be able to get access to the data, irrespective of whether or not the underlying data was for a legal or a natural person.

So if one looks at it from a pure SSAC concern about security and stability, if you have security practitioners who are trying to track down some information and they're accredited and they're operating under appropriate rules and they're -- you know, there's accountability and auditability and everything, it should not matter whether or not the data belongs to a legal person or natural person. And it should not be an issue for them, but it has been. I'm reporting here that it was a major factor in the discussions. And, as I say, in trying to introspect and understand what's driving that, it was the identification of the sort of hidden

force behind the system, behind the discussions, which is that that's all that anybody is expecting to be able to get access to.

So that's the -- that's the message, a fairly forceful message.

Next slide, please.

So within -- so within the scope of the working group, we did recommend that the distinction between legal and natural persons be gathered and used -- there are a lot of, as I say, specific detailed issues about all of that. But it's probably not necessary in this setting to go into those details. Simply that's a useful discriminator, but as I say not the totality of what needs to be done. Thank you.

Next slide.

So this recommendation moves to the second big question that was taken up within the working group. On the surface, the question was: Is it feasible to use pseudonymous email addresses as a way of making it possible to send messages to the registrant of a domain name without disclosing what their real address is so to give them a sense -- to give them a degree of privacy and at the same time a degree of accessibility.

And the idea of pseudonymous email is a different email address that translates in a one-directional way so you can't untranslate it into the real address of the person.

Again, digging under the surface, there really were two very distinct objectives that were tangled up with each other. One is exactly what I said, which is how do you provide access to registrants in a way that preserves their privacy and, yet gives access?

There were a couple different ways that you could do that. You could simply have a forwarding service by the registrar. You could have a Web-based system, which some registrars do. So the question then is, well, why this intense focus on pseudonymous email contacts?

Turns out that a second and entirely separate objective for some people is the desire

To correlate registrations in which -- again, from mostly from a security perspective but perhaps for other purposes, you want to be able to see a whole set of registrations and see that they are correlated with each other in the sense they have the same registrant. Don't know who it is. Don't know what their email address is but you know that they share in common this handle, this descriptor.

Well, oh, my goodness, that's interesting, but that is an entirely separate and also completely unrelated aspect.

If you're really going to try to do that, it's one thing to do it across the registrations within a single registrar. It's an entirely different thing to try to do that across all of the registrars or even all of the contracted party registrars.

It's a much more complicated and technically demanding issue. But it also turns out that, again, if one stands back and looks at this from a sort of common-sense perspective that it's the same problem in a different guise.
If you had access, appropriately controlled and authorized and so forth, to the entire range of registrations, there are plenty of ways to get correlated information. Not only by using email addresses but by using other factors as well.

So, again, the reason for the focus on this particular question of feasibility of pseudonymous email is an attempt at a solution to a problem and it's sort of the wrong problem and the wrong solution. The problem is -- that's underlying this is: Well, if I can't see all the data even if I'm authorized to do that, well, then what are we going to do in the meantime? And the answer is: Why don't you build a system that gives you access to the data you need to get to and do that in a way that makes it actually work for everybody?

And once you do that, then the two questions underlying this, how do you protect the privacy of individuals you're going to contact and how do you correlate common properties across registrations, become disentangled and are entirely separate and distinct questions.

The next slide.

MERIKE KAEO: All right. Thank you, Steve, for that very thorough and detailed context. I know that there's been a lot of discussions in the community and also with the board regarding the SSAD and the ODP.

And I would welcome also all SSAC members to attend the Thursday session that will give an update on the SSAD ODP.

But at this point, I would like to ask my board colleagues if they have any questions or comments regarding SAC118 and want to elaborate a little bit more, discuss, and get some clarifications.

GÖRAN MARBY: So I'm starting to think -- thank you for the presentation, Steve.

It's subtraction.

I wonder sometimes if there's any way we can reach -- you -- SSAC gives advice based on the security and stability of the Internet within ICANN's mission, et cetera, et cetera.

The problem here is we have -- we do -- the WHOIS would have been open if the European Commission didn't mess it up. Sorry for saying that, but that's actually the truth. And I hope this is recorded.

I have no opinion about the GDPR as a legislation as itself, but I think we all see the drawbacks of it.

And sometimes I think that we -- it's like we need to find a common reality how to define the problems that this actually did.

The law is -- the law is -- it's like a Swiss cheese. It's very hard in some places and a big hole in other ones. And that is what I -- these holes also creates a lot of discussion.

We're getting more case law as -- almost every day, because GDPR is proven -- is proved in European courts. And it has, of course, an effect on all the Internet users around the world. Because sometimes it's even hard to know who is a European citizen who owns a domain name.

And you made some comments about it, about the SSAD. We can always discuss those as well.

And the discussion about natural legal persons. We have received, for instance, already back in the day -- I think it was 2018 or '19, we received guidance from the Data Protection Board, which is the official people who talk -- who make recommendations about this. And they told us how to look at the question about natural, legal persons.

And, of course, they are the one -- And there has been some case laws after that that might affect it. But they still gave the advice.

So I'm just thinking sometimes on how we can -- how we can -- with respect of your competence in what you do -- and (indiscernible) has talked about this several times, I think. How do we -- Is there any way we can sort of -- without having the debate, that I go and tell, yeah, but the law says this in this chapter, and this is how we interpret it, and I can prove the evidence for that, because the European Commission (indiscernible) asked to (indiscernible) a law that changes some of the basic facts, et cetera, et cetera.

If there's any way we can reach this common reality about what we think -- I'm not adverse to the proposals you're making. It's just that the -- and I'm not even a lawyer. But I have -- we have worked -- the PDPs has worked very hard to understand. If there's any way we can maybe find some common ground. We don't think -- I don't think that the problem is huge. You point that, that

-- the retraction of data from the WHOIS system. I've been public on the fact that I think that the -- some of the decisions made by the cause of WHOIS is not beneficial toward the transparency of the Internet and creates havoc for researchers, I.P. community, and other ones.

That's not -- I think we all agree on that one.
But I think we need to find this common ground somewhere to talk about it.

This is a -- this is a -- it's a -- And it's not only Europe. Because of the privacy shields discussions, as you know, and I call them differently, where the E.U. has to make an agreement with a country about actually transferring data. Many countries who would like to have these kinds of exchanges with the European Union countries now are entering trade agreements, really, with the European Union, which means that they have to have, according to the setup, GDPR-like legislation. So it's not only GDPR that spreads like a virus, in a sense -- that's a very bad analogy right now -- it's also the legislation itself is spreading by -- I mean, it's discussed even here in California, in order to have international data transfers.

So I don't -- I agree with Steve, you know. And your competence about this is much higher than I have ever been. I just wonder if there's a possibility for us to find this common ground. Let us at

least stake down and say, okay, this problem we agree with, this problem we don't agree with, so we don't end up with the -- it's like someone just said in the GAC meeting I just heard that the -- SSAD should be able to give anyone who grants a request sort of an answer. SSAD cannot do that, because it's against the law. And having those discussions -- it's -- I don't think it helps us at all.

Sorry. I should shut up and give it to Becky, who is a lawyer, and, actually, a really good lawyer when it comes to GDPR.

MERIKE KAEO: Yeah. So thank you very much for that, Göran.

So I think, Steve, unless you want to reply immediately, I'd like to give the floor to Becky and then see whether or not from the SSAC side we have any replies.

STEVE CROCKER: You're in charge.

MERIKE KAEO: So, Becky, please.

BECKY BURR: She is in charge, isn't she? That's great.

I just want to start out by saying, Steve, everything you said made total sense. The problem is we are dealing with a world in which -- it doesn't make total sense.

And we found ourselves in a situation that at a certain point in this discussion where it became clear that ultimately, because we could not get actionable advice from the European Data Protection Authority, ultimately the decision to disclose information was going to be situated in the hands of the registrar, of each individual registrar, and they were going to be to make it on the basis of their interpretation of the law.

And once we got to that point, I'm just going to say now in total hindsight we should have stopped and thought about what the implications of that realization were.

I think we did get to that point, but then we just plowed forward on the theory that somehow we would be able to address all of the concerns and all of the completely perfectly rationale -- I mean, you are absolutely right. The distinction between legal and natural is irrelevant for someone who needs to get the information for legitimate purposes. There are, you know, any number of things that in a perfectly rationale world we all could have sat down and resolved. But we are dealing with a law that is extremely unclear in a world in which we cannot get actionable advice. And so I think from a security perspective, one of the

things we need to think about is sort of what is it that is actually needed in the first instance?

Is there a way to get to totally, aggressively, pseudonymized information that works for security researchers in a different way than the SSAD is going to deliver? I mean, the SSAD is going to deliver one thing and one thing only which is it's going to deliver a uniform intake system. It is not going to deliver predictable results on the outside, on the outcome. It is not going to deliver -- it may deliver more timely results but probably not timely enough for anybody. But predictability and reliability are unobtainable in a world in which in the end we don't know what the law means, and we must defer to the registrar in most cases to determine what the law means for them.

So you and I have talked about this in any number of circumstances, Steve. Every single thing you said made sense except in the context of the law that we're dealing with.

STEVE CROCKER: So maybe I'll offer up three comments.

First of all, I very much appreciated your comments about the realization that if there was a problem and maybe if you had seen that, you would have stopped earlier. And my response to that is, yes, and it's not too late to stop now. And in particular, I don't see

how to listen to that comment and we're going to push forward with SSAD anyway.

Since this is being recorded, we might as well take advantage of it and put it on the record. SSAD should be stopped cold now. It is not fit for purpose. It is not a solution to a problem. Haven't defined the problem properly and so back up and start over. So that's one comment.

Second comment is I hear you and Göran very clearly about what you think the impact of the law is. I think it's important to back up and examine the assumptions very, very clearly.

This is not the right time. We don't have the right setting and we certainly don't have enough time and preparation. But I think there is a quite serious discussion, sober and careful and measured discussion, to have about what the assumptions are and all of that.

Third thing that I want to say -- and then I will stop -- is there's a huge value in solving pieces that can be solved as opposed to trying to solve everything at once.

The structure of the problem space has some parts that should be relatively easy to make progress on and other parts that might be hard. And there is a lot to be said, I think, for subdividing the

problems and working on the ones that can be solved and then letting experience and time and other pressures come to bear so that you can then deal progressively with other pieces of the problem space.

So those are the three things that I would like to offer to you.
And just a quick recap, SSAD is an incomplete solution to the problem and plowing forward with it is just, you know, throwing good money after bad, in a way.

GÖRAN MARBY: Can I ask you, Steve: What do you think is the biggest problem with the SSAD system?

Sorry, Rod, for rushing in.

STEVE CROCKER: Well, it's exactly what you said, Göran. It passes requests on and there is no uniformity, no certainty, no clarity as to what's going to happen with them.

It used to be that when a request was made through WHOIS, you would get a response back in, say, a second, give or take.

We have on the record a statement by a very reputable and serious registrar who says, Look, we give back responses now in

three days and we think that's fast enough. We think that's pretty good. If you do the arithmetic, that is 100,000 times slower.

Now, what systems in this world do you use where somebody can insert a factor of ten to the fifth delay and then claim, Well, it's just a slight delay? That's nonsense.

So we're assembled here as the Board and SSAC. I will just comment that one of the attributes of SSAC is that we're fundamentally a technical body. So in addition to the specific issues of security and stability, by and large, each and every one of us knows something about designing and operating systems, to greater or lesser extent. And whatever the impact is on the security researchers and security practitioners that we're speaking on behalf of, the more fundamental thing is that we're being presented here with a design that simply fails basic fundamental sanity check as to whether or not it's a useful system.

MERIKE KAEO: Oops, I'm on mute. Thank you very much for the discussion. I do see Ron has been patiently waiting with his hand up. And I see Maarten's hand up as well and then Becky. I don't know if Maarten or Becky was first. But let me give the floor to Rod first.

ROD RASMUSSEN: Thank you, Merike. Thank you, Steve. Between Steve and Patrik, I have very large shoes to fill. I am not going to attempt to do that at the moment other than to point out that we have had a lot of discussions around these topics and issues, et cetera. And kind of the system as proposed right now solves part of the problem, as any partial solution that's ever been put out there, finds a lack of uptake in its usage and the consistency in being able to get a response out of something without any assurances of that in a time amount of time, et cetera, or likely to lead to lack of adoption. That seems like a lot of time and energy spent on not solving the problems.

And that takes me to the point I wanted to make when I raised my hand, which is I think that when you have spent a lot of time trying to adjust and come together to figure out how we can solve all the problems that have been caused by introduction of GDPR and other privacy regimes into this world and step back and say: What are the fundamental things we want to accomplish as a community? Do we as a community agree that it's important for law enforcement and security researchers, at least in our bailiwick and more broadly other folks with legitimate interests of being able to access that data, do we all agree that it is important to provide a way to do that in a legal manner obviously? And we all agree to that. I don't know that we're there.

I think we kind of implicitly say that. We have not spent a lot of time saying here is our manifesto of what we need to be able to do and then take that to the appropriate authorities if the law is in the way or technical folks, if it's hard to implement or work with operational folks if it's expensive to implement. What are -- as Steve was saying, get back to basics a bit and maybe approach this in a way that we can all come at it from a unified perspective of what we want to accomplish.

I will just add that to what Steve had to say as a potential way forward. Thank you.

MERIKE KAEO: Thank you very much for that added context, Rod. I think very useful to hear.

Maarten, you're next.

MAARTEN BOTTERMAN: Yeah, no, for sure. I appreciate the discussion and the input.

The challenge is the difference between the one second and the hundred thousand times that is that it's not only -- it's not answering the same question. It's a question that has embedded quality of service of doing things that the law requires, a balancing test and all the legal risks that come with it.

So whether this is the system that's going to work, I'm sure with all aspirations we will get closer to the answer. And this will also require GNSO to also reflect on it. But the points you make about the necessity of security researchers having access is, of course, an excellent point and we can see how to resolve that.

But, yeah, the problem is not automated system. The problem is a law that doesn't make clear answers possible, I think.

But, Becky, you know much more about that.

BECKY BURR: So I don't disagree. I think there is a problem with the law, but I do think that it is worth stopping and sort of taking a step back and acknowledging what I think Steve and I agree on, which was at a certain point we should have realized that fundamentally what was possible given the direction that we were able to get from the European Data Protection Board, which was very little, was going to leave this in the hands of individual decisions.

And so I just want to say I completely -- I am completely sympathetic to the notion that we may have proceeded down a path on the hope that this would deliver things that people wanted when, in fact, we should have stopped and said: Here is exactly what is going to be delivered, which is an intake system

which doesn't -- which does not guarantee anything on the out -- on the other side.

Now, just to be clear, ICANN org went to heroic lengths really, heroic lengths, to try to explain what was needed to essentially propose a model where ICANN would itself conduct the balancing test, where we would have gotten a predictable model. And we were not able to get uptake on that from the European Data Protection Board or from the European Commission.

But I just don't want to lose -- I mean, I -- I mean, we're in the ODP phase. We are going to look at all of those issues that we have to look at as a Board with respect to whether the public interest is being served, whether we are fulfilling our fiduciary duty with respect to what's being delivered.

But I don't want to lose sight of the fact that maybe we need a -- maybe we need to think about -- we need to have a way to think about sort of what's being delivered and what it's going to cost in the middle of the process as opposed to at the end of the process. Maybe we need to have a way to think about sort of fundamental redirection issues in the policy development process.

I just think that there's a huge amount to be learned from the experience that we have all had with respect to the development

of the EPDP phase 1, phase 2, phase 2(a). And I don't want to lose sight of that going down the road.

MERIKE KAEO: Thank you very much. I think this is an extremely important discussion to have so that, you know, all sides and all of the different aspects really can be articulated. I mean, this is not very easy. Finding a solution obviously is not easy. So I very much appreciate the frank discussion on both sides.

At this point in time, we have five minutes left.

GÖRAN MARBY: Can I steal two minutes of them because I want to go back to something Steve said, the assumptions.

I think that's an important thing to say. I mean, we live in a world where laws makes a difference.

And I understand better now what your intent is with the discussion. It's just that it came out as a problem with the SSAD. I mean, your problem is with the law. I'm sorry to say that, because if the law wasn't there, we wouldn't have this discussion. We would have the opposite discussion, I would suspect, but we wouldn't have this discussion.

STEVE CROCKER: I'm going to interrupt, Göran. In your office a while ago, quite a while ago now, we had a version of this discussion. And my reaction to what you said then, which is essentially what you're saying now is I don't think that that's true. I don't think that the law per se is necessarily the problem.

The law is -- the GDPR and its various cousins, the California version and so forth, are motivated by a very sensible desire to protect the privacy of people, which is a perfectly sensible thing.

The particular embodiment of it, the particular interpretation of it and so forth is where things get to be very complicated and messy.

But the underlying motivation of those laws is something that basically we're all supportive of. How to fashion workable systems -- and by "systems" I'm talking about not only electronic systems but also the bureaucratic systems that we build for ourselves and the processes that we engage in -- is a challenge that is our bread and butter collectively. That's the job that we're engaged in.

And I think that it's a perfectly sensible challenge. It's not as complicated as solving world hunger. It's not as complicated as even solving pandemics. It's just a system-design problem. Not

going to be perfect, but it does not have to be as bad as this one is.

So that's my attempt at pushing back about challenging the assumptions. And to say that the trouble is all because of that law, I think, is where the difficulty starts and the path past that point is sort of unrecoverable, if that's the position that we take.

And I just plant a marker and say that does not seem to me a terrible thing that the law as stated is all that burdensome. It is in general a positive thing.

But it does require a lot of work to figure out how we're going to achieve all of the other desirable things, not only from a security and stability point of view but for all of the other uses that that data needs to be used by.

Thank you.

GÖRAN MARBY: I vividly remember that discussion when we traded examples with each other. The contracted parties as the data controller have the data and according to the law, they make the balancing test. They have the legal responsibility for making that. They can delegate it to someone, but they still have the responsibility to do it.

According to the formats from the European Commission, the registrant can go after anyone in the chain so that's why I sometimes call it (indiscernible).

But you see, with all the respect, I think to build the system, it has to be adhering to the law. I'm a privacy person. I have my credentials in that.

I was the one who personally took and made sure that the Data Retention Act in Europe was taken to the European Court of Justice to be taken down. There's not a question about that.

But WHOIS was open before GDPR came around, and we have received over the years several papers from the Data Protection Board both as the Article 29 and after the Data Protection Board was formed guiding us how to look at the specific issue about WHOIS, including talks about natural and legal persons, how we have to disclose data, how to work with balancing tests, all public.

I mean, I think we should just take that into account when we look to a solution because if we can't define the problem together, Steve -- and I remember you looked at me and said: Are you telling me that we need to have a contracted party to make that decision? And I said yes. And that is how the law works like.

That's why I think instead of trading legal things, let's have a conversation where we actually go through this assumption. I'm willing to bring external legal counselor so you can don't have to listen to me all the time. We have experts that worked with the EPDP in the form of Bird & Bird and Jones Day. Let's have the discussion instead.

There is no -- I went out very early on and said that I think that the implementation of the GDPR will have an effect on transparency of the Internet. And it will have an effect on data researchers. It will have an effect -- and I think that's not good.

The European Commission, the Data Protection who wrote the law, the European Union as the members states all adhered to that. And we asked them for: Why don't you declare this is a public interest for member states because that will take away the problem. We didn't get that.

We asked them why this is a different from the trademark database. They said, Oh, it's very different. It's an E.U. institution. We asked them to give us the mandate to make the balancing test. They said no. They haven't said anything, to be honest. We tried every avenue in my thinking to get better advice for the WHOIS.

To be honest, Steve, I don't think in the balance -- and that's an argument we probably haven't been good enough to do. In the balance of what they believe is the importance of privacy of registrants combined with the needs for you and researchers and law enforcements, they think that the privacy goes first. That is the intent of the legislature.

Do I think that is right or wrong? I'm not having an opinion about it. But that's where we are, Steve. And that's why I think let's have a discussion together about the assumptions. And there are more lawyers that can fix -- who can talk about this as well.

MERIKE KAEO: So thank you very much, Göran.

And we are at the top of the hour. I am extremely grateful that we had this conversation, especially the very forthright conversation. And I am going to end this session on a little bit of a different note because I want to just simply say that it has been my privilege to act in the role of SSAC's liaison to the Board. And I'm extremely thankful to both my SSAC and Board colleagues for their support.

I also want to welcome Jim as the new incoming SSAC liaison to the Board. And I can unequivocally say that from the transition period in the last few months, I know he will be an effective liaison.

Thank you to Board ops, SSAC support staff for keeping me on the straight and narrow. And I just wanted to say thank you to all of you.

And with this, I close out the Board-SSAC session. Thank you very much.

MAARTEN BOTTERMAN: Thank you, Merike, for all you've done for all of us. Looking forward to seeing you around. Thank you, all.

ROD RASMUSSEN: Thank you from the SSAC as well. You did a fantastic job.

LEON SANCHEZ: Thanks, everyone.

MERIKE KAEO: Thank you.

MAARTEN BOTTERMAN: Thanks for the discussion.

[END OF TRANSCRIPT]