DANIELLE RUTHERFORD: Welcome, everyone, to the SSAC Evolution of the DNS Resolution Work Party held on Thursday March 31st 2022 at 21:00 UTC. Barry, over to you.

BARRY LEIBA: All right. Well, definitely owing to the IETF week last week, I certainly have not done a lot of prep for this. And Russ and I did not get a chance to talk, which we should do before the next meeting. But what we had was the charter being reviewed by the SSAC plenary, and I have seen no comments about it.

RUSS HOUSLEY: Yes. We got crickets.

BARRY LEIBA: So I think we have a charter. Andrew, what say you?

ANDREW MCCONACHIE: Oh, I get to have an opinion? There was absolutely nothing sent in. I get notifications whenever someone makes an edit to one of the Google documents that I own, and I got no notifications on this one. So, nothing.

BARRY LEIBA: Okay.

RUSS HOUSLEY: So we got no edits and we got no e-mail.

BARRY LEIBA: And I take silence as approval in that case. Are we through the review period, or do we still have more time for it?

RUSS HOUSLEY: No, it was supposed to end yesterday.

BARRY LEIBA: Okay. That's what I thought but I wasn't sure I had it right. Okay, then I think we have a charter, and what I guess we're looking for on this call is for us to get started on discussion of what we're actually going to say in the document where we actually want to go with it with a goal of coming up with an outline of the document.

Rod, I see your hand.

ROD RASMUSSEN: Yeah. I'm just going to confirm your declaration of charter because we've had reminders and plenty of time. And I know people are playing attention since we had comments coming in on other things. Did anybody take a look at it who's not in the work party? Hard to know. Right? But this was the opportunity for folks to do so. So, yeah, let's move on. I re-reviewed it, and I didn't have anything to change.

BARRY LEIBA: As did I, so okay.

RUSS HOUSLEY: Cool. All right, so I guess the real question is, who wants to do what first? Ultimately leading to those things Barry said which are like a document and an outline.

BARRY LEIBA: So let's kick off a discussion. Would anybody like to talk about their favorite thing that they want to put in this document? And I'm seeing crickets here, too.

GEOFF HUSTON: It's such an open-ended question, Barry. It's unanswerable.

RUSS HOUSLEY: Okay, let's look at the deliverables, then, which are down a little further. [inaudible].

ROD RASMUSSEN: Can somebody repaste the link? Because I lost my tab with that one on it, and I came on a little late. To the charter, thanks. Thank you.

RUSS HOUSLEY: So, "produce a report that analyzes the effects of relevant new technologies." So which ones are relevant?

SUZANNE WOOLF: One way to approach it is to take the idealized brief overview of the simplicity that was once the DNS protocol and database and then walk through each section of that and say, "Oh, by the way, this is more complicated now because the following extensions to the protocol or practices of operators ..." And take from there. So what are the impacts of this? What are the impacts of the changing ways that resolvers are deployed or the implications of having applications choosing their own resolver? And separately, all the namespace questions and DNSSEC or lack of.

So if we think that that's a sensible breakdown for some of the new and extended technologies, we have to be clear on how do they change the simple model and what's the impact of that.

BARRY LEIBA: Okay. Geoff.

GEOFF HUSTON: There's another paper circulating around that Kalinski wrote in Verisign, I suspect with a few conspirators inside Verisign, about the increasing obscurity and the evolution of the DNS if you look at the whole issue of taking a formally, relatively open protocol and open interoperation and obscuring it as a deliberate evolutionary step actually allows us to see less and less of the operations of the infrastructure.

So studies like NCAP crippled from the start [inaudible] don't see very much anymore. And the whole issue is the infrastructure of the DNS is now almost impossible to perceive in any meaningful way because of this loss of coherence.

And now, this is almost an academic paper—Burt Kalinski's paper. This is, "Oh, the woes of the world are manifold and various, and here are a few more woes." There are no solutions here. But that's sort of where it's leaning. And if we're happy to write "o tempora, o mores" kinds of papers, then this might well be another one.

But it is a very real issue because those twin concepts of an increasing sensitivity over how much the DNS betrays individuals and privacy, and an increasing issue that the only way to make evolutionary change in the DNS is to tunnel through crafty old crap by encrypting it to make sure middleware doesn't tamper those two things combined.

It's kind of an interesting document, but I'm kind of wondering how much more can we say that Burt Kalinski hasn't said already. And I'll hand it back to you because I've got nothing more to say.

RUSS HOUSLEY: Okay. Rod.

ROD RASMUSSEN: So an approach that I was envisioning way back when was taking a look at the impact on various parties and different types of entities and people throughout the DNS ecosystem on this evolution. So thinking about impacts on end users, impacts on resolver operators, and impacts

on authoritative operators, impacts on DNS registrars and registries. There are different things that this evolution stuff implies.

I think that we talked about this a bit in the DoH/DoT thing. There is this interesting shift if we're going to start saying applications will use their own unique protocols and maybe their own unique naming systems to talk to to get to a destination to get content that, yes, it hides this infrastructure from various parties along the way and provides challenges to those who are trying to manage a naming system or protect their trademarks within a naming system or something. Kinds of impacts like that.

But it also provides this centralization in uber control/visibility to those who are running this custom infrastructure to know everything about the people who are in the applications and the processes that are using their unique naming DNS-like thing. So I think there are some interesting things we can talk about from the perspective of you may be thinking you're evolving towards this private utopia where nobody can spy on what you're doing. But at the same time, you're actually handing the keys to everything you're doing to some third party that you now trust, and you don't realize it.

BARRY LEIBA: Yeah. Kind of along with that, one of the things that I was thinking is that as we look at proposals to do something like putting DNS records into blockchains and stuff like that, we're moving from where the authoritative servers have the definitive information about the DNS and we ask them for it to where clients can just go directly to a database and

retrieve the information themselves rather than going through any sort of recursive resolver or authoritative source. The blockchain becomes an authoritative source.

What does that do to the DNS resolution system and the namespace? And what are the effects that that has? And that's something I would like to spend some time looking at.

Warren, you've put your hand down. Do you ...

WARREN KUMARI: I was just wondering. The comment that you're now handing all of your information to a third party. I'm a little confused by that because I thought that's what you are doing anyway as soon as you start using the DNS. Unless you're running your own resolver, you're handing all of your information to whoever does the resolving.

ROD RASMUSSEN: A different third party. We'll put it that way.

WARREN KUMARI: Yeah.

BARRY LEIBA: I think a lot of that gets down to, whom do you trust?

WARREN KUMARI: Right.

BARRY LEIBA: Whom do you want [to give your] information to? Some people say, “Google is more trustable than my ISP.” And some people say the other way around.

WARREN KUMARI: Yep. And that’s why—

ROD RASMUSSEN: I’m looking at the logical extension of ... I downloaded an app from an app store. And, I don’t know. It's an app. Right? [A little] [attention] to who the developer is. But that developer is using a custom resolution system, so it’s just interesting.

WARREN KUMARI: But you’re trusting the application developer. I would posit that actually having the application do its own resolution means that now you're only trusting one person—the app developer—instead of the app developer and whoever happens to run your DNS. But anyway, that’s getting, like, we’re trying to solve the document now [inaudible].

ROD RASMUSSEN: Yeah, exactly. I think there are interesting things to explore there. Let’s put it that way.

BARRY LEIBA: Yes, I agree with that.

ROD RASMUSSEN: I think there are some interesting things to explore on the governance side of that, too. We have a governance model. Whether we think it's useful or not, or broken or not, is a different discussion. But we do have a governance model today where, in theory, the Internet's identifiers have responsible organizations managing them and making sure they're allocated properly and if there's funny business going on, that there's some sort of resolution towards whatever the funny business might have been.

And you're moving to a world where you've got individual [inaudible] organizations making their own rules that you have to live by or, in the case of blockchain and some of there other things, the rules are completely different. There may be no resolution to the issue that comes up. So that's an interesting area to explore, too.

BARRY LEIBA: Geoff.

GEOFF HUSTON: My apologies. I hadn't stopped thinking about the technology side before it got maneuvered over by Rod into governance issues, etc. There is a bunch more to say on the technology side, and part of it is the hidden advantages of querying authoritative servers all of the time actually has a lot to do with the timeliness and the control of the timeliness of the information that the DNS "publishes."

One of the strong things about the DNS is that it doesn't need revocation. It doesn't need to, if you will, have a mechanism to cancel stuff that would otherwise be good because you can control the timeline of that validity, and therefore you can unsay things by dint of TTLs because folks are meant to query.

But if you change that with pre-provisioning/preloading and distribute the answers, you're not necessarily going to be able to distribute the time control of that information. And part of the more generic observation about evolutionary structures here is that by optimizing the little bit that they think is worth optimizing and improving/evolving, how much of everything else is being hampered or otherwise devalued because you've changed that essential property?

And there is this tension between on-demand caching versus just-in-time delivery from authoritative sources that sits inside all of these mass distribution mechanisms. Do I send out information in advance, or do I wait for people to pull?

RUSS HOUSLEY: This goes back to the argument between operating system developers, between capabilities and [ackles]. It's the same issue. Right?

GEOFF HUSTON: Oh, it's a competing science issue. Yes.

RUSS HOUSLEY: Right? It's exactly the same issue, and we're reliving it in PKI, the difference between long-lived certs with revocation or short-lived certs. Right? It's the same [issue].

GEOFF HUSTON: I love the way you say "revocation" as if it actually works.

RUSS HOUSLEY: Oh, we're [inaudible]—

GEOFF HUSTON: My hat's off to you, but I am laughing and falling off my chair.

RUSS HOUSLEY: It's the [plain tension], though.

GEOFF HUSTON: But nevertheless, that tension ... Yes, you're quite right. It's very, very generic. But each time we talk about evolution of technology, we kind of forget it. It's kind of like, "I'm optimizing X." Yeah, but what about Y? "No, I'm optimizing X. Let's don't have the Y discussion." And it goes on and on and on like this. It's worth mentioning, you know, because as we try and shave milliseconds off of the DNS, what you actually tend to lose is currency.

Now back to blockchain.

BARRY LEIBA: Warren.

WARREN KUMARI: I guess I'm just going to say that different people are optimizing for different things. Right? The people who are optimizing for "let's cache the hell out of this" are optimizing for a specific use case. And that might be a valid use case. Right? Surprisingly, the TTLs that Google sets on its authoritative DNS records were not chosen at random. So there is ...

I think we just need to be careful not to sound as though we're trying to teach our grandmothers to suck eggs, or similar. People who are optimizing for resilience have a different set of incentives than those who are optimizing for agility and a different set of incentives than those who are optimizing for response time.

GEOFF HUSTON: I agree with that, but we've seen the DNS almost as a single playpen with a global set of operating characteristics with a single imposed behavior. A caching resolver can cache any name. It treats all names the same. The only difference is the suggested TTL that comes with the data.

But when you talk about this, Warren, and you kind of say there are a whole bunch of different reasons why folk want to optimize different names in different directions, the underlying issue is, is the existing infrastructure sufficiently capable or do I have to bend the infrastructure? And if I bend the infrastructure, am I bending it for

everyone or just for this use case? And what are the implications of that?

WARREN KUMARI: Yeah. The underlying infrastructure clearly could be way better and could be more flexible. But then again, it is by far the world's largest and most reliable distributed database. It has warts, but it is surprisingly unsucky. But anyway, this is just a rathole and navel gazing, I think.

GEOFF HUSTON: Well, it would be. But there are some quite fundamental changes in the way it operates being not only contemplated but pushed out there.

WARREN KUMARI: Sorry. I guess I was meaning us discussing it now is [irrelevant].

GEOFF HUSTON: Oh, okay. Yeah. But I still think this is a computer science-styled academic paper. You can't say that DoH sucks and we should never ever use it. That's not a rational outcome. It's very hard to be judgmental about any of this.

WARREN KUMARI: I fully agree because as far as I can see, DoH is just encrypting to whatever resolver you've chosen. I think that there's a fundamental bit that I'm not understanding here. You're encrypting your DNS thing so a monkey in the middle can't look at it.

This is something that could be done anyway, before. And if you didn't like you network admin looking at stuff, you could have just fired up a VPN or Tor or anything else. So I think I'd keep being mystified by the few that it's actually doing anything different. But maybe things will become clearer to me as time goes by.

ROD RASMUSSEN: Well, that monkey in the middle may be somebody who's doing something positive for you. Right? So ...

WARREN KUMARI: Well, sure. But if that monkey in the middle is something doing something positive for you, presumably you would want to expose your information to them. And so you should be ... Either by using MDM profiles, enterprise profiles. Using them as your resolver.

ROD RASMUSSEN: Sure. [inaudible] you've got this really cool popup from Chrome or Firefox saying, "Hey, click on this thing to protect yourself from getting hacked or spied upon" without you know that that was going to show something else [off]. That's the downside of the ...

A lack of awareness by end users is what the implications of them making technology choices is and marketing people exploiting the hell out of that.

WARREN KUMARI: Yeah. I mean, I should point out once again that was a Mozilla thing.

ROD RASMUSSEN: Yeah. I've certainly got [inaudible] my Firefox, "Please turn this on. You're [not] safe."

BARRY LEIBA: But to go a bit off on what Tara said in the chat. She said, "Just a matter of scale now." Yes, exactly. You could always do this, but just about nobody did.

WARREN KUMARI: Apart from Chromecast and Netflix, YouTube for a short while on some things because they didn't work well. And [inaudible].

BARRY LEIBA: We've seen it mostly in content delivery networks, right. But now with what DoH is doing, it's making it easy for any application to build in its own. And is that changing anything? Maybe the answer is that it isn't, really, because, as you said, you could have always done it.

WARREN KUMARI: Yeah. And I think maybe going through again and look at hope many thing did. Maybe just the scale of how many things were already doing their own resolution anyway. But if one looks on GitHub, for example, you see a huge number of things had already built in their own resolver. But anyway, once again trying to run the [buff] now.

BARRY LEIBA: Anyone else? Other discussion?

So I see nobody really jumped on my "how do applications directly accessing the data rather than going through authoritative servers change things". We've had not discussion about that angle of it. Is that not something that we think is interesting?

ROD RASMUSSEN: Oh, I think it's very interesting from an end user impact. How do I troubleshoot something? And if I'm an ISP or a recursive resolver operator for a large set of customers who've downloaded some app that's now doing something different and they're getting weird results, how do I deal with that?

BARRY LEIBA: Yeah.

GEOFF HUSTON: Or how do I troubleshoot that application? Equally, and this is that blog that we talked about that Warren and Burt Kalinski—Warren, too—are writing about. How much do these things stop us doing any kind of meaningful introspection about the DNS? If it's all obscured, what's left? You can't diagnose. You can't understand. You can't see. It's all just packets in the dark.

And every programmer is perfect, and every program works the way it's intended. So why are we obsessing about the problem here. Right?

BARRY LEIBA: Yeah.

GEOFF HUSTON: There is this implicit assumption, and DNSSEC is almost a gigantic instantiation of the assumption that there is one DNS. One key. One root of trust. One trust anchor. One source of authority. One thing.

And the evolutionary pressure tends to be, in various ways and forms, fragmentary. And at an abstract level, they obviously come into some kind of conflict at some point down the line. What we thought was one actually requires [inaudible] applications to use the platform resolver, the platform resolver to use the ISP resolver, the ISP resolver to use the authoritative DNS infrastructure.

We have all this terminology, environment, expectations, etc., around unity and cohesion, yet we have a whole bunch of folk understanding that their optimizations invariably try and break aspects of that unity and cohesion. And in so doing, we tend to lose sight of what it was in the first place, and even lose sight of what the changes are. We just can't see them anymore.

Yeah, there are a few unanswerable questions out there. How many queries per day? And the answer is, "Define a query." I can't. "Well, I can't answer you.

BARRY LEIBA: Define—

GEOFF HUSTON: [inaudible]. [Thanks, Tara]. Yeah, right. I get the sense that what we see are a bunch of small changes that we think are big, and we'd like to flag them as, "Well, these are worth attending to. These are worth flagging. These are worth saying something about."

But at that point, we kind of go, "Well, what are we going to say?" And it's sort of, "Ugh, ugh." [And that certainly]—

WARREN KUMARI: I still think that one of the biggest things is the increasing likelihood of things using not the DNS to do resolution. And to me, that seems much more of a security, stability, and reliability/existential threat to the DNS and ICANN.

BARRY LEIBA: Yeah, I—

WARREN KUMARI: And the other one which, I guess, I don't know if we want to talk about is what seems to be an increase in the number of attempts to use the DNS to either do censorship or force people to go to specific content. But I think that might be outside the scope. But then again, it is also quite related to evolution of how the DNS works. But whatever.

SUZANNE WOOLF: Well, it kind of is, Warren. Because, as in the simple world we started living in so long ago, DNS couldn't be used that way. So rather than change the nature of what governments and large organizations do, they've been changing the DNS, which is not really all that surprising, but is ...

I think that what you just said is an example and a symptoms rather than an unrelated observation.

BARRY LEIBA: And I certainly think that what Warren was just talking about is something that I want to spend some time on, on this paper, in the work party discussing.

GEOFF HUSTON: I'd also like to bring up the SVCB record because—

UNIDENTIFIED MALE: Ugh ...

GEOFF HUSTON: Yeah, right, ugh. Because what's going on is that the DNS is now becoming a rendezvous protocol, not a machine name to machine IP address protocol. So it's no longer a mapping. You feed the profile of a service into the DNS, and you get back the precise credentials and

parameters you're going to use for the next packet you send. [inaudible].

WARREN KUMARI: Wasn't that already something that kind of tried to happen with SRV records and it didn't fly?

GEOFF HUSTON: No, no. It hasn't happened overnight, Warren. We've taken steps in that direction for some years, but nevertheless there it is. And oddly enough, if you thought that the DNS was a personal privacy leak in the past, if you really think hard about HTTPS and SVCB records, this is the predictor of the immediately next-millisecond future for every single user.

And all of a sudden, those privacy issues and so on become quite disturbing but alarmingly accurate. This is not just about you. It's about exactly what you're going to do next. And that evolutionary process that packs more information into the DNS also then packs more risk because that information is now not just in aggregate—I know what Warren does—but in the microscopic—I know what Warren's going to do in the next millisecond because I saw his DNS query for an SVCB record. So I know the next packet.

WARREN KUMARI: That feels like it might be a bit of a job to me. I personally think SVCB is already a crappy idea, but that's a separate thing. I don't know if—

GEOFF HUSTON: It's a separate debate. It's a thing. Crappy or not, it's a thing. I've got the same plumber coming back, so I'm going to just drop out for a second.

SUZANNE WOOLF: Good luck.

BARRY LEIBA: Those plumbers. Warren, you have to stop sending the plumbers to Geoff's house.

WARREN KUMARI: I wonder if he saw my previous note on my [inaudible].

BARRY LEIBA: [He probably did].

SUZANNE WOOLF: [Who is it]?

BARRY LEIBA: Okay, so let's start looking then at how we want to structure the document. What are the things we want to put into the guts of the document? Obviously, we're going to have the Executive Summary and the Introduction and background stuff, but what's going to go in the guts here?

WARREN KUMARI: I think we should start off with what I believe Suzanne suggested. Maybe it was someone else. That first we start off with, "In the beginning there was the void and the void was empty. And then somebody said, 'Let us make the DNS'. And it was simple and it was good. And then people added all sorts of crap on top of it."

SUZANNE WOOLF: That's a very colorful way to put it, Warren. But yeah, that's pretty much what I suggested. And just go through, okay, what has been layered on top of this and that and the other thing.

BARRY LEIBA: All right.

SUZANNE WOOLF: I mean, that's what I've thought of so far. Geoff, didn't that make your day?

GEOFF HUSTON: I think it might have.

SUZANNE WOOLF: Quotes from ... Hey, Warren quoting Genesis.

GEOFF HUSTON: Yeah, I know.

SUZANNE WOOLF: But, yeah. If it turns out that it doesn't work as a way to organize what we're trying to say. The other this is, what are we trying to say? Are we trying to say this should stop? Are we trying to say people should understand it so they can deal with it?

BARRY LEIBA: Yeah, I think the latter, that these are the implications of this so that we can avoid negative consequences from some of it if awareness helps us with that, so that we have information about deployment considerations and things like that. At least that was my thought on putting this work party together. That that was what we were trying to do—give advice to implementers, give advice to deployers, operators; give advice to anybody who is going to be affected by the implementations we're talking about once we figure out what those implications are.

ROD RASMUSSEN: Perhaps even policy makers—aah!

BARRY LEIBA: Perhaps policy makers. Yeah, the interesting thought there is ...

GEOFF HUSTON: There is also to give advice in terms of evaluation by consumers/users/policy makers.

BARRY LEIBA: Yeah, sure.

GEOFF HUSTON: If you're playing with fire, the answer is, well it can heat your house and burn it down, too. And there is a critical distinction in evaluating what the naked flame is going to be used for in terms of its benefits and dangers. And that's, I think, where we're heading here.

It's not, "Stop there. Don't do that." But more, what new risks are we introducing and what are the benefits we're introducing? And how can we evaluate these kinds of changes as consumers of this technology?

BARRY LEIBA: Yep, agreed.

TARA WHALEN: I like the way Suzanne was talking about—

GEOFF HUSTON: But who's the audience for that?

TARA WHALEN: Go ahead.

BARRY LEIBA: No. Go ahead, Tara.

TARA WHALEN: I was going to say I like what Suzanne's talking about with the evolution because you were talking about ... There are differences in functionality that have evolved over time. And I think there are a lot of different decision points. You're talking about consumers. There are decisions that different players in the system have been making about what you can and cannot do and what is available to you. And you may not be getting the result that you think when you are setting some set of configurations.

Things may be changing between you and the endpoint in which maybe you don't have all the powers that you think. And if we sort of are talking about all of the different features and configurations that are happening as these queries are working their way through the system, that might help, I guess, maybe to highlight some of the places where there are risks and change in expectation.

SUZANNE WOOLF: The other thing that I think has been a big evolutionary force is that nobody likes simple in the modern Internet. They want it to be perfect or they want it to be flash or they want it to be faster no matter what they have to do to get there. And I think simplicity is undervalued, and that's another pressure.

BARRY LEIBA: Interesting observation. Warren.

WARREN KUMARI: I have no idea what I was going to say. Oh, yes I do. So Geoff's thing on making sure that people are informed, etc., who exactly do we think the audience of that is? Do we think my auntie is going to read this and be like, "Oh, it had never occurred to me that changing my resolver to use 1.1.1.1 is going to make Cloudflare know what I ordered for lunch"? Or is it more to inform policy people so that they can inform the users [inaudible]? Who's going to read it?

+ BARRY LEIBA: I look at it more as the latter. That the ISPs will read it. The policy people will read it. You know what I say about trying to educate you auntie. I bring this up many times that people who don't have the technical background ... We can explain things in a non-technical way to them, but trying to educate them on highly-technical things just isn't practical.

Geoff.

UNIDENTIFIED SPEAKER: [Well put].

GEOFF HUSTON: No one's in charge. No one's going to read this. There is no one to evaluate and make a decision. This is all market forces. But as soon as I say that this is all market forces, what I'm really talking about is that this

is all a bunch of folk who think they understand what's going on, making decisions in their own self-interest that affect everyone else. What we are trying to do is to help this aggregate market be a little more self-aware about the pressures that are being placed upon it because I can't and you can't rely on regulatory intervention anymore.

The regulators are scared stiff about this stuff. No one thinks that they have a controlling say anyway. But we're also scared stiff that an untrammeled, unfiltered, undistorted distorted market is actually going to work against the interest of consumers in the long run. It won't be a valuable tool anymore. And so trying to gently assist folk to think carefully and make good decisions is the best that any of us can hope for.

So who would read this? I would hope some folk in Google who were product managers. I would hope some folk in Comcast who are product managers and looking at this stuff. I would hope some academics. And that's about the best I could hope. And some policy makers on the extreme end.

BARRY LEIBA: Right. My goal here is to make sure that the people who are making those decisions of, "Well, this is my best interest," at least also have the information about the affects it has so that they can balance that.

WARREN KUMARI: So let me just jump in. I'm not entirely sure that I agree with Geoff that this is all being market driven and that the regulators are scared of this

because the majority, or a large amount of many of these changes are being driven by things like the IETF. And that's because the market does it. It's because a bunch of somewhat liberal folk in the IETF believe that having governments read your e-mail is sub-optimal.

There is a fair bit of people doing this because they believe that the security win is important of the end user. And a lot of the people participating really believe that they are there to serve the interests—especially security interests—of the user.

Yes, that happens to also possibly be good for their employer because it's good for Apple and Google, etc., if users feel more comfortable using the Internet. But from good's standpoint, DoH and DoT, etc., are simply a cost from a purely business thing. Google wants to do it because it's good for the user, but it has cost and has nothing that can be sold, really. And I'm sure I worded that badly.

But I think the "it's purely market driven" might be giving the impression that there's a product being sold. And yet I know somebody going to say if you're not being charged for it, you are the project. I don't know what I can do other than point at things like the DNS privacy statement once again attest to the fact that I am stating that we are strictly following them and it's not being mined or monetized, etc. But I don't know how I can convince people of that in any other way.

GEOFF HUSTON: But if the aim here, Warren, was to convince the IETF, we're the wrong people in the wrong room.

WARREN KUMARI: Yep.

GEOFF HUSTON: Let's all invade DNSOP or DPRIVE or whatever, and have that discussion inside that working group and see how far we get because it's a one-sided conversation filled with proponents who never see downside easily. And I say that after, like the rest of you, many decades of brutal experience in various roles. Like everyone else here.

SUZANNE WOOLF: Now, really. I didn't think we were talking about cryptocurrency and blockchains. Come on.

GEOFF HUSTON: All I'm saying is that it's a tough crowd to have an even debate on.

SUZANNE WOOLF: No, no, no. I'm agreeing with you, but [inaudible]—

WARREN KUMARI: But I think we [inaudible].

SUZANNE WOOLF: —canonical example these days.

WARREN KUMARI: We also have to be careful that it's not that we're sniping from the sidelines being like, "You folk over there are doing the wrong thing." If we think they're doing the wrong thing, then ...

GEOFF HUSTON: [inaudible]. I thought it was more a case of calling out in a little bit of a deeper sense of what we see. That's all. I hesitate to use words like "right" or "wrong" in this kind of situation. I don't think they add any value.

WARREN KUMARI: Okay. I did get the impression that there was some "this DoH thing is an abomination unto man." Wow, apparently, I'm all in scripture mode today. And, you know, we the people on this—

GEOFF HUSTON: [I think] it's in your head, Warren. I honestly think that's in your head. [inaudible].

WARREN KUMARI: It could be. Could be. Okay. Maybe I'm just overly sensitive because I've had this fight before with so many people on the conspiracy theory of that.

BARRY LEIBA: Okay. Are we ready to get a summary and wrap up the meeting for today and think about what we're going to talk about next week? I think we are.

GEOFF HUSTON: Absolutely, because I'd be keen to see anyone try and figure out what we said in this [last one]. Go for is, Andrew. That's your job.

BARRY LEIBA: Russ, your hand is up. And then Rod.

RUSS MUNDY: Yeah. Thanks, Barry. Before we actually started the meeting, I said there was one thing I wanted to just throw out to the work party so the work party could think about it as your SSAC liaison to the RSSAC. And we did discuss this a little bit in the joint meeting of RSSAC-SSAC we had last ICANN meeting.

I did point out that this work party was just getting underway. There was no current decision about whether or not any external experts would be invited. It just simply isn't mature enough yet. But what I had said recently to the RSSAC folks is that perhaps by ICANN74, the work party will have progressed sufficiently to decide whether or not they wanted to invite any external expertise.

So it was really just to let the work party know that I'd said this and go from there, for whatever it's worth. That's it. Thanks.

BARRY LEIBA: Okay. Does anybody have any comment directly on that, about whether you think it might be useful to have other people join our conversation or part of it?

WARREN KUMARI: I would think that it might be useful, but I think that we should wait until we are much crisper on what we're actually doing and have started some work, etc. [inaudible]—

BARRY LEIBA: Oh, yes. Sure.

WARREN KUMARI: —[figure out] who actually and how and what. Because at the moment, it's ... Yeah.

BARRY LEIBA: Oh, way too early right now. We're just batting ideas around. Rod.

ROD RASMUSSEN: Right. So my suggestion at this point would be to have Andrew and/or Danielle go through what we said today in our notes and perhaps get the big bullet items that we can then organized next week into an outline of a paper.

BARRY LEIBA: Yes, that's a good hope. Andrew, do you have sufficient notes to steer us in that direction?

ANDREW MCCONACHIE: I think I can come up with some high-level topics that we can expand on for our next meeting.

BARRY LEIBA: Perfect.

ANDREW MCCONACHIE: Do Russ Housley and Barry want to have a meeting before this meeting, like a quick catch-up call?

BARRY LEIBA: Yeah.

ANDREW MCCONACHIE: Do we want to catch up via e-mail? How do you guys want to handle that?

BARRY LEIBA: Russ had to drop off for a conflict, but Russ and I will be talking early next week. Do we want to do that with the Admin Committee or should be just do that by ourselves for right now?

ANDREW MCCONACHIE: I wouldn't do it with the Admin Committee, but if you want me to join and have a standing meeting, we can do that as well. I would do that for the routing security admin call. They typically last like 15 minutes, and it's just a good time to touch base before the actually work party call.

BARRY LEIBA: Great. We will include you in setting up the call next week.

ANDREW MCCONACHIE: Okay.

BARRY LEIBA: All right, then I think we have ... We thank you for the discussion this week. Warren, your hand is still up. Is that your old hand?

WARREN KUMARI: Yeah, it's an old hand.

BARRY LEIBA: Okay, thought so. Just wanted to make sure that I wasn't leaving you hanging.

WARREN KUMARI: Nope.

BARRY LEIBA: Okay, then I guess that ... Thanks, everybody, for the conversation this week, and we have a good starting point for putting together some topics for talking about next week.

WARREN KUMARI: Thanks, you all.

BARRY LEIBA: Thanks for coming.

[END OF TRANSCRIPTION]