ICANN85 Mumbai | CF – SSAC Lightning Talks (2 of 2)
Tuesday, March 10, 2026 – 9:00 to 10:00 IST

KATHY SCHNITT

Thank you. Hello and welcome to the SSAC Lightning Talk session. My name is Kathy and I am the Participation Manager for this session. Please be advised that this session is being recorded and is governed by the ICANN Community Participant Code of Conduct, the ICANN Expected Standards of Behavior, and the ICANN Community Anti-Harassment Policy. Regarding participation today, this session is primarily designed for the internal work and discussion of SSAC members.

To join the speaking queue, SSAC members must be logged into Zoom and use the Raise Hand feature. When called upon, please state your name for the record. For observers, please note that the comments or questions in the Zoom chat will not be read aloud. However, the chair of the session may invite questions from the audience at their discretion and time permitting. Now I'm happy to hand the floor back over to Barry Leiba.

BARRY LEIBA

Hi, I'm Barry Leiba. Welcome to the second and final session of SSAC Lightning Talks. As Kathy said, it's my discretion and I will allow questions from non-SSAC members, time permitting, but everybody please use the Zoom tool for raising your hand. Danielle will run the queue based on that. We have three good talks today

and I'm not going to waste any more time babbling. So, there he is, Steve. You're up doing Project Jake.

STEVE CROCKER

I'm always nervous about the interaction of the too many channels here. Thank you, Barry. So, this feels like coming home. I've been on a mission, which you're going to hear about in some detail in a second, dealing with a very long, long standing set of issues related to WHOIS and DNS registration data. And it's a pleasure to be back among the original.

My entry into the ICANN business was this group here. And so let me just say that I've got two objectives here. One is to tell you what we've been doing. And the other is to actively ask that any comments, thoughts, questions, whatever, and advice, I'm completely open to either here now or at any time over time. And so, with that, I'll start.

So, we have a project called Project Jake, which is dealing with a sort of fresh framework for dealing with both the collection and the disclosure of DNS and not just DNS could be numbers as well, registration data. So, with that, allegedly, I've got control here. Let's see what happens. Why? It says I'm sharing my screen.

BARRY LEIBA

Steve is in control of nothing.

STEVE CROCKER

That's the button I'm pressing. And it was working a minute ago. Oh, maybe I wasn't -- okay, good. So, just a little brief of history. The DNS registration data has grown over the entire lifetime of networking from the very beginnings in an Ad Hoc

and unplanned way. And the origins go back to the ARPANET days when time-shared computers were connected as hosts on the network. That's prior to the internet.

That's prior to the domain name system. That's prior to the World Wide Web, just to take you back to ancient times. And the original numbering system on the network was blazingly simple. UCLA, where I was host number one. SRI was host number two, and so forth. Very quickly, we decided it would be nice to have some names for these numbers.

And so, we invented very complex names. UCLA seemed good for us, and SRI seemed good for SRI, and we had short strings like that. So, that was before the invention of the domain name system. Over a relatively short period of time, the amount of information related to these hosts grew to a sizable corpus. It was useful to have a contact person.

Basically, it's the sysadmin role. In other words, sysadmin hadn't been invented yet, and became the technical contact for who's running the other hosts. And an administrative person that you could appeal to in case somebody needed attention at an administrative level, like diddling your machine from afar that you

didn't like and you wanted to know who to call. You scale anything up by a factor of a million, and the structure changes a little bit.

So, Jake Feindler, Elizabeth was her name, but she went by Jake, has gone by Jake all her life. She's still around. She's an old lady, but she was the keeper of this corpus of information at that time, and a really delightful person. Still has all her marbles. It's really quite amazing. Anyway, so she allowed us to use her name for this project.

We've taken a fresh look, as I said, at the whole business of both collecting information and disclosing it. Today, if you ask, so how is this done? In the ICANN environment, you'll hear about the registration data RDRS request system, which is you get to log into it and make your request. It only goes to the contracted parties. Most of the CCs are not involved.

And then it gets sent over to them, and then you log out, and you wait for a response. How does that response come back? It comes back by email or something like that. It is, what's the technical term? A rinky-dink system. It's really crude how it was put together. There's a history behind all of that, but it's painful.

I was on the Board for a long time. I was chair for several years. And when we hired a new CEO, Fadi Chehadé, I said, let's see what we can do to fix this. Passed a formal Board resolution in November of 2012, if I recall. And on the basis of that, he structured a expert Working Group, which produced a 150-page report. Very good

stuff. Not perfect, but very, very good stuff. Board does not make policy. Everybody knows that.

We handed this report back over to the GNSO, who promptly set it aside, started over, ran into the ditch again and again. So, when I left the Board, an embarrassingly long, what, eight years ago, coming up on eight and a half years ago. I was essentially retired and did not have another agenda. And this thing gnawed at me.

So, I gathered a handful of people who shared the similar frustrations that I had across all the spectrum, across the business and the technology and the political aspects. And we're deeply knowledgeable, all the names that you would recognize. And we began to talk offline, no portfolio, no funding, anything.

And after a while, got some, the idea started to get cleaner and cleaner. And then we said, okay, now we've got to go communicate this. That means we've got to get some help. That means we've got to get some money. It means I've got to have an organization to put the money in. All right. So, we did it. So, we created a small non-profit and we got a small amount of money and we've been pushing on that.

And then several months ago, after not getting much traction, anybody wanting to do anything, a group showed up that said, this is the right idea we want to play. The group was the TWNIC. They run the Taiwan top level domain and very, very sharp, not only technically, but they understood all of the bureaucracy and politics of it all. And so, we've been pushing on a pilot, which is, it's up and

running, not perfectly yet, but we're getting there. And very quickly, all the pieces are falling in place.

So, that's what I wanted to share. And I'm going to tell you now, what the basic elements are. And focus primarily on the disclosure process.

The environment we're working in, in the whole internet, is that you've got two negative forces that have come into play. One is a huge abuse of registration data evolved over time, spam, harassment, et cetera, et cetera. And a counter reaction leading to trying to make that data unavailable, either by lying about it, putting in false data, one, two, three, even Mickey Mouse Lane in Disneyland or something, or using proxies to hide it. Or now with government action, raising privacy to a very high level, GDPR being the primary instance of it, but not the only one, there's privacy regimes all over the place, state of California, notably, among others.

So it's like a big pendulum swinging way over on the privacy side, but the pendulum, the image you should have is the pendulum is like a wrecking ball. It swung hard, but it didn't improve anything. It just changed the balance. And so, you've got other differences. So, our approach is this, we said, okay, so what's the common sense of it?

From a business point of view, if you just look at it like a business operation, you have large numbers of requesters who are making the same kind of request over and over again, because they're

dealing with the same issues. And the decisions about whether to disclose that data and who to and all of that is basically repeatable. So, we said, why don't we take advantage of the commonality?

So, we talk about groups of requesters that have similar needs and behave similarly, willing to be accountable. And we talk about groups of data holders. We use the term data holder as an umbrella for both registrars and registries, because if you look outside of the ICANN contracted parties and look at registries around the world, in some cases, and TWNIC happens to be one of them, you have thick registries that are the primary interface point for requesting data, which they get from their registrars, of course.

So, we talked about groups of requesters, groups of data holders, and agreements between those groups in advance of making specific requests. So with that, we've designed a system, and here we go. So we've got, I'll skip over all this stuff and basically cover all of this, and I'll show you the pictures.

So, we have a design. The lower left is the place to start where a requester is running software, and with that software can make a request to data holders. Superstructure on top of that to put all of the agreements in place. So, a process for creating groups, for adding requesters, for forming agreements. And then with all of that in place, a requester can make a request authentication of who it is with an identity server run by the group of requesters rather than being a general-purpose thing, but using the same protocols that one uses in these areas.

Part of the agreement is that OpenID server run in an acceptable way and under appropriate controls so that you can trust it, et cetera. The underlying protocols is RDAP with enhancements. RFC 9560 covers most of it, and then further enhancements on top of that. That's another picture.

One of the things that emerged over our entire process is that different classes of registrants might want to be treated in different ways. Typically, one makes a distinction between businesses and individuals and provides a different level of protection for individuals than for businesses. But there's no reason that's the only distinction.

In working with Taiwan, we said, so what are the distinctions you actually make? Turns out they have five. Why five? Well, there's businesses versus individuals, and then in each case, whether or not they require extra privacy. So, that's four. And then a fifth one emerged recently that they have some registrations that come in from certain registrars where it's not the privacy that is a distinction. It is what level of validation the data has been subjected to.

They use green to indicate that has nothing to do with ecology or saving the planet, but a green registration from their perspective is one where the data has been subjected to extra validation on the inbound side.

We have some tools. The picture that I was showing you before are the operating tools for making requests and responding to it. We

also have tools for documenting what level of validation and what level of sensitivity has been assigned to each data element. This is a snapshot for an individual with extra privacy. This is a snapshot of a normal business registration.

I'll flip back and forth, and you can see on the right-hand side large changes in sensitivity level, which is what controls the privacy. And then this is the normal business, and here is a green registration. And I'll flip back and forth so you can see the middle column is where the validation stuff shows up.

Here's an example of different levels of access to the same data. The stuff on the left is with a very low level of access, and so there's a lot of redacted stuff that's highlighted in red. And the same registration data disclosed properly for somebody with higher level access. And there are benefits, and we're ready to talk to people. Did I make it?

BARRY LEIBA You did, and you even have a minute or two for questions. So, are there any questions showing up in Zoom? Nothing in Zoom. Well, talk for another minute then. I'm sorry? Talk for another minute then.

STEVE CROCKER No, I'm happy to, as I said at the opening, happy to talk to people. We are semi-actively recruiting others. I say semi-actively because we've got a lot of work to do with what we have, but basically

looking forward to engaging others. We're working with TWNIC as a data holder. We're working with two organizations that are not in a position of being formally announceable, one in the law enforcement area and one in the intellectual property arena, who will then speak on behalf of others.

So, it's not just a single agency, but ones that speak on behalf of others. And all of that is moving forward, and I look forward to providing further updates, both to SSAC as desired directly, and more of this stuff will become public.

BARRY LEIBA: Okay. Well, thanks for telling us about it. And the next slot is Georgia Osborne will talk to us about WSIS+20.

GEORGIA OSBORNE: Excellent. Thank you so much. So, many of us are familiar to WSIS at this point. You've probably seen quite a few webinars so far. So, this is going to focus on a little bit of a different angle. So what it actually means for security, stability, and resilience going forward. So, why do we care? Why do I care?

So, this presentation will observe the outcome document as a set of signals on security, stability, and resilience of the particularly the internet infrastructure. ICANN also help to facilitate a series of meetings and small discussion groups to hear and share thoughts on WSIS+20 and ICANN84 in Dublin last year, and we're key in presenting the voices of the technical community in this area.

And there are elements of the document that appear to be stabilizing, but also elements I will outline that remain ambiguous and have implications for security, stability, and resilience.

There may be future points of pressure that emerge in regard to the DNS and wider SSR issues, which I will bring to this presentation. So, I'm not going to go into what is WSIS. Hopefully we will know, but just in case you don't, I will just give a very brief overview. And so, the World Summit on the Information Society is UN-mandated process that sets the high-level political vision and governance principles for the global internet and digital corporation, including how governments, the private sector, civil society, and the technical community are expected to interact with each other.

It took place in two different phases, in Geneva in 2003 and Tunisia in 2005. And WSIS essentially created the political legitimacy for the multi-stakeholder model, which is why it's relevant. So, it's one of the foundations in which ICANN's legitimacy rests. So, the WSIS+20 review outcome document reaffirms the original principles, but also it updates them for AI and data governments. And it also signals where future political pressures may emerge that will affect SSR going forward.

So, one thing about the SSAC is sometimes there seems to be a theme of cats. So, in staying with that, I have tried to keep on that. Of course.

BARRY LEIBA Everyone, pick your favorite cat.

GEORGIA OSBORNE So, first of all, the outcome document did have some stakeholders breathing a sigh of relief. It reaffirmed the multi-stakeholder model. The technical community were explicitly recognized. Here, I want to recognize the work and the voices from our own community here in ICANN and beyond, but also the technical community coalition for multi-stakeholderism.

The Internet Governance forum was also given a permanent mandate. So, the outcome document has stabilized some areas of Internet Governance, which does reduce short-term uncertainty. The IGF being made permanent is a success for those who support its mandate. However, it may also reduce or alter any urgency for evolution of the IGF. It also introduced more of a focus on government-to-government dialogue within the IGF ecosystem or enhanced cooperation, which risks two-track deliberation.

Continued use of this phrase, enhanced cooperation, in this context could present a risk with the focus on more of a government-to-government dialogue. Meaning that just like what was discussed in the plenary yesterday, the journey to support multi-stakeholderism isn't over. So, the outcome document also acknowledges the importance of developing digital public goods and digital public infrastructure. For example, you can see here in paragraph 17 of the outcome document, which explicitly calls out

the importance of Open-Source software, open data, and open AI models, open standards, and open content.

While fragmentation is named as a risk in the outcome document, prevention mechanisms are not strengthened. Perhaps to those familiar with the process and WSIS, this is to be fully expected. So, there's no binding commitments against fragmentation, no operational definitions, and no technical guardrails.

Fragmentation is recognized, but the document relies on cooperation rather than any particular detail on safeguards. It's important to note when the language is ambiguous here, it will be up to the technical community to define and fill in those gaps.

The outcome document stresses the importance of refraining from internet shutdowns, as seen in paragraph 76. Shutdowns normalize state intervention at the network layer, which further increases the fragmentation risks.

Again, noting that the language around the mechanisms, definitions, and safeguards remain weak. The outcome document acknowledges some challenges around stability, security, and resilience, including in paragraph 16, 21, and 27, which recognizes the gaps and inequalities that persist between those who remain unconnected or do not have adequate access to the internet.

The financing gaps are also recognized in paragraph 65 to 67 and highlights the creation of an assessment mechanism. However, while these challenges are acknowledged, they perhaps lack the

clear technical direction or detail to provide adequate solution, and only time will tell.

The outcome document raises the importance of the significant efforts that have been made by stakeholder communities to build confidence and security and to protect infrastructure services, transactions, and other digital services from the rising threat of malicious activities and physical risks to infrastructure. However, with the previous two slides, they also emphasize that there are key capacity gaps, and capacity gaps here can have the potential to equal attack surfaces.

WSIS+20 is the first-time data governance and AI appear as a dedicated section with explicit interoperability language, so it's no longer just about privacy or trade. It's about system coherence. The language is deliberate. It signals concern that divergent data regimes could undermine cross-border services, distributed architecture, and global technical coordination.

Paragraph 109 notes the establishment of the Office for Digital and Emerging Technologies with an expanding role for the United Nations Group on Information Society, or UNGIS. They are designated to coordinate WSIS and the GDC, or Global Digital Compact, impact of the future to produce joint implementation roadmaps and to improve system-wide coherence.

This is a shift from mainly loosely connected forums to a more synchronized UN digital architecture. In further centralization like this, there could be potential for further risk of consolidation of

agenda setting away from technical domains, so coordination does strengthen resilience when it amplifies technical expertise, but there is a potential to weaken resilience when it substitutes for it.

Technical expertise is going to be even more significant, and the need for technical voices might increase going forward if there's an increase in centralization with the absence of technical expertise within that space. So, I just want to highlight that the points made here, they aren't conclusions, but they can be seen as signals.

WSIS+20 stabilized institutions, but not the underlying politics. Fragmentation, internet stability, and resiliency risks are recognized, but remain under-specified. Although the under-specification and lack of technical detail may be expected by many, these are the gaps that will likely need to be filled by the rest of us, and to that end, the technical voice remains essential, and probably increasingly so.

I will just end this presentation by saying that the theme that I've picked up on personally so far in this ICANN85 forum is the importance of stability and resilience in the internet ecosystem in uncertain times. Thank you.

BARRY LEIBA Thanks, Georgia. While we wait for people to raise their hands, do you have any sense of whether the outcome document will result in any real effect with respect to shutdowns, gaps, and inequalities, or is it just a few words on a piece of paper that will drift away?

GEORGIA OSBORNE So, I might do the classic thing of not directly answering that, because I do think there's an element that time will have to tell, because I'm not going to predict the future, but given the way that these documents have happened in the past, I guess there's a sense that there is some success, that multi-stakeholderism has been sort of amplified by this, but it doesn't feel like enough, and there's still a long way to go. And in terms of real protection for stability and resilience, I don't think I can say I feel confident enough that it will provide it.

BARRY LEIBA Thanks. Danielle, do we have any questions in Zoom?

DANIELLE RUTHERFORD Do we ever. First, we've got Steve Crocker and then Tara.

STEVE CROCKER Thank you. Just a clarification. When I hear the word fragmentation, I think of packet fragmentation, but that's not what you're talking about, right? You're talking about pieces of the Internet separating and being unreachable from others who are like that. Thank you.

BARRY LEIBA Just to note, there was a lot of head nodding going on in the room.

DANIELLE RUTHERFORD All right, Tara, and then we've got a writing question from Ram and then Rick.

TARA WHALEN Thank you for that, Georgia. You had a data governance slide, and I wondered, did you have a sense when people talk about, I guess, different regimes, you talked about different kind of handling regimes. Is the motivator there a lot about facilitating cross-border data for purposes of commerce as a driver for unified, or how much support is there for, in a sense, unification of strong data protection, which is a very different thing?

GEORGIA OSBORNE That's a great question, and I think for us here in this multi-stakeholder community, it's hard for us to see the thought patterns and the thought processes of the UN process, which is multilateral, so country to country, government to government.

So, really, the kind of element that you were sort of pointing out there, which is the kind of multi-stakeholderism, the business, the industry, the technical community are slightly more absent from there, and it's really up to the governments to hear those voices and bring that to the table in the data governance piece there.

DANIELLE RUTHERFORD All right, I'm going to read a question on behalf of Ram Mohan, regarding fragmentation being left to the technical community. How is coordination happening? What role does the SSAC have?

GEORGIA OSBORNE Well, I'm not going to speak on behalf of SSAC here, but what I will say is that we provide a lot of technical advice that I think will be useful going forward, and I hope to continue to be useful. I think technical voices are becoming even more important in this dialogue to provide the right guidance for those who do have the say to pick up, pick up, and the way that we communicate that advice is going to be paramount to this.

DANIELLE RUTHERFORD All right, and he has a second question. Does the advent of Hyperscalers and widely deployed GPT engines result in further centralization and concentration?

GEORGIA OSBORNE So, I think it probably does, and I will leave that there because I think that's quite a complicated question.

BARRY LEIBA Does the word AI appear in the document, and how many times?

GEORGIA OSBORNE I try not to mention that word in this room.

DANIELLE RUTHERFORD All right. Next, we have Rick Wilhelm.

RICK WILHELM Thanks, Georgia, for doing this difficult task. I would, there's, I'm looking forward to going back through the slides because there's a lot to take in in a very short time, but one of them that I was struck on the prior slide about section 120 or paragraph or 121, this one in particular didn't really, this one was sort of depressing when I read that, that like I read it and I read it and I read it a third time, and every time I read it, for me, it got worse, and I'm not asking, it's not really a question unless maybe is that, or is there an alternate reading that if we were having coffee you might say to me, no, Rick, actually, this is actually super positive. I think you're interpreting it wrong, but like I read this and I'm like, oh thanks.

GEORGIA OSBORNE I like your take on it, Rick, but…

BARRY LEIBA It's very well-articulated.

GEORGIA OSBORNE I think how you view this will be in the eyes of the beholder. Some people might cry for joy at this and others might be in despair. I think part of me wants to be very positive going forward, that we will continue to have those technical voices and the kind of the

mixture of people and it not be so centralized in a space that might miss out important aspects, diversity of thought, of opinion, and the kind of technical ability needed to provide that. But again, I feel the same. Robert.

DANIELLE RUTHERFORD Robert?

ROBERT GUERRA Thank you, Georgia, again for a great overview and great visuals as well. I just wanted to get your thoughts on a couple of things that are a little bit troubling for me and kind of your advice is that on one hand you mentioned there's a need for ever greater technical expertise, yet at the same time a shift towards more enhanced cooperation.

And so, if that's the case, what are your thoughts on where the tech community voice would be most effective and have it preserved and not shifted to more institutional for like the ITU, where it's harder to have access to documents and other things?

GEORGIA OSBORNE Yeah, I think this is going to be a question that we will be tackling. I think for me personally, the importance comes from communicating that technical advice effectively to the right people. I think occasionally, and I say this as somebody new, so I hope nobody attacks me here, occasionally, and I think this goes

for any community, the technical community or any community has a tendency to stay within their group and not reach out.

And I think the importance of reaching out to those other groups, bring in very effective communication on quite complex technology so that the right people and the policymakers and those who will be at the table making those decisions have what it takes to be able to come forward so that enhanced cooperation includes the right people as well.

BARRY LEIBA Do we have a final question or are we done? Oh, then I'll just thank you, Georgia, and I'll leave you with a request that next time, how about alpacas?

GEORGIA OSBORNE Absolutely, I can do that.

BARRY LEIBA And now it's time for the Warren and Gautam show. Hit it. Gautam says with much fewer cats.

WARREN KUMARI Yeah, for some reason, I don't think we have any cats in this, which is, I know, I know, I have failed you all. We should so have done that. Why weren't you here earlier? So, first off, a quick note. A couple of us have spoken to ICANN about being able to do wildcards in TLDs, and ICANN generally seemed supportive, but

they said, oh, hang on a second, we wouldn't be allowed to do an RSTEP or similar on this because there's existing SSAC advice that says you can't do this, and that's one of the drivers for this. So, we brought this along to SSAC, Gautam and I, for consideration. So, that's the background.

So, what are we talking about? Well, currently in the ICANN registry agreement, there's a prohibition on wildcards. Basically, what it says here, the use of DNS wildcard resource records or any other method or technology for synthesizing DNS resource records is prohibited.

So, what actually are wildcards and what are we talking about? Well, here is an example of a service called RSVPify.com, and the purpose of this is if you're setting up an event, like in this case, a 21st birthday party, you can go to RSVPify and set up a certain account with them and announce your event and then send out links to all of your friends. When your friend clicks on a link, they can click a button saying, yes, I want to come to your party, that sounds really cool.

If you look at the URL, I had to make it bigger because it's really small in that image, the URL is 21stbirthdaysparkinganewdecade.RSVPify.com. So, basically for my 21st birthday, obviously my 21st birthday, the event name is baked into the URL. So, what happens if somebody goes to something that doesn't exist? So, for example, if I went to imadethisup.RSVPify.com, well, instead of it just not resolving,

somehow magically, I still get to RSVPify.com, but it says there's no such event here. And any domain name at RSVPify.com, you get to the same page.

So, how do they possibly do this magic? Here is an example of looking up some string that doesn't exist at RSVPify and it resolves. The way that they do this is through wildcards. There are actually two different types of wildcards, as you could probably guess from the ICANN text in the registry agreement.

There's actual real wildcard records themselves, which if you put in your zone file, it's asterisk dot, in this case, RSVPify.com and an IP address. Or what's more common is synthesized answers. Any query that shows up. Why'd that break? Did I drop off Zoom? I'm, my Zoom seems to have disconnected. I will share again. It came back. There we go. And now there's an echo. Anyway, my speaker's off. It's not me. Okay, there we go.

The way that most of them are actually implemented is with synthesized answers where the authoritative server, if it gets a name that it hasn't, that's not configured for other use, we'll just make up an answer on the fly. So, basically the authoritative service synthesizes answers.

So, this works in RSVPify, but are these actually common in the wild? It turns out, yes, they're really common. Here are some, I looked at the top thousand domain names and a lot of them have wildcards. So, for example, bing.com or Shopify or Reddit or GitHub user content, Google APIs, Visual Studio, right? These are

all large, well-known properties. And all of these second level domains have wildcards in them.

So, presumably the issue isn't really that wildcards in the DNS are an issue, right? What's the actual issue here? Why is there a prohibition? Well, some history. Back in around 2003, a large registry stuck a wildcard in their TLD. This was designed to provide useful search answers if somebody went to an unregistered domain. So, for example, if somebody went to, the TLD wasn't actually travel, but for example, if somebody had gone to Rome.travel, if Rome wasn't actually registered, it would take them to a cool search page with a bunch of useful information like flights to Rome or hotels in Rome or similar.

At that time, there was a fair bit of pushback for some fairly reasonable reasons at the time. There was the potential for phishing issues. So, if somebody had gone to a domain name that didn't exist, this would take them to the search page and potentially there could be phishing stuff there.

Potential lesser privacy. If somebody mistyped a domain name, instead of only linking, leaking that from the resolver to the authoritative, because the domain name would suddenly look like it existed, the user's browser would connect and that would expose their IP address, their browser, cookies, et cetera. It also had some negative consequences for spam detection. A fairly common anti-spam mechanism is when mail arrives from a domain, the anti-spam system looks to see if the domain name exists.

In this particular case, if there's a wildcard, every domain in that TLD would look like it exists. There're also some other concerns like how does this work with other protocols, et cetera. So, there was some good reasons for pushback for doing that at the TLD level at the time. And it led to a bunch of documents, including three of them from SSAC.

Basically, redirection common net domains, why TLDs shouldn't be allowed to use resource records, and a recommendation to prohibit the use of resource records in TLDs. Some other interesting stuff is actually Trillions asked to be able to do this in and it was declined because of the SSAC advice. And finally, it ended up in the ICANN registry agreement, officially prohibiting them.

So, the question is why is this okay for something like RSVPify, but not for a TLD? Well, the thing that's different between a TLD and a service like RSVPify or Reddit or Bing is a TLD has multiple registrants in the zone. Things like Reddit don't, Bing don't, Google APIs don't.

So, TLDs have multiple registrants. However, brand TLDs don't. Brand TLDs by definition have a single registrant and are under a single entity's control.

So, what's my point and why are we talking about this? Well, if one was able to do wildcards specifically in brand TLDs, you could potentially make these be a lot more valuable. So, for example, and I'm using Google properties here as an example, instead of having

www.youtube.com/c/veritasium/videos, you could give the Veritasium channel something like Veritasium.youtube. That's nicer and easier to remember. It's shorter. I mean, it looks more attractive. This is not a technical argument. This is a fair bit of this is around, you know, making URLs look nicer.

Instead of having www.google.com/map/places/221BBaker Street, London, blah, blah, blah, blah, blah. You could give users something like Sherlock.maps. User could say, you want to find my house? It's my username.maps. You know, Gautam.maps would tell me where Gautam lives if he wanted to share that sort of information.

This would allow brand TLDs to actually be useful and valuable. So, Gautam and I are sort of asking the SSAC to revisit the earlier advice. We've actually got sort of draft text, which we think might be worth considering. But we think if this were to happen, there should be some very strong restrictions to avoid all of the security issues that the original prohibition is for.

First off, this would only be allowed in a single registrant TLD, basically like a spec 13 brand TLD. We also think that this would have to do something like point at a service, not a website. So, using the example of like YouTube, it would point at the service that's run by YouTube. So, the content that there is not directly under the user's control.

Another example of this could be iCloud. If it was wkumari.icloud, it would be my iCloud drive, but it wouldn't be the HTML that I set

up and create. The reason that it shouldn't be able to point at a straight website is this was designed to things like cookie theft and super cookies or phishing pages. If you allow it to point at arbitrary HTML, users could put up phishing pages and they could create a lot of these.

The litmus test basically is the wild card, as I said before, don't allow it to point directly at user provided HTML. Instead, it would have to be something like a service in the same way that Reddit, when you go to whatever. reddit, it takes you to a page under Reddit's control. some of these other ones are more sort of opinions.

I personally think no MX records. I think it would be weird to allow email to Bob@Veritasium.YouTube as an example. That feels like it blurs the line and gets back into the potential for confusion. I think also the TLD would have to do DNSSEC and HSTS preload. Luckily DNSSEC is already required. I think HSTS preload is just a general best practice.

So, when I mentioned making brand TLDs be actually usable, useful, this is from the dns.coffee graveyard site and it lists 150 TLDs which have been withdrawn or terminated or failed. And basically, all of them that have failed have been brands, right? Like .Bentley, .Comcast, .Old Navy, Volkswagen. That's because generally brand TLDs haven't been that useful for the organization because they're not really usable for anything interesting. And so, thank you. And hopefully there are a bunch of questions.

BARRY LEIBA And how would you enforce the restrictions, particularly number one? Technically or procedurally?

WARREN KUMARI Through ICANN contract. So, when somebody says I want to have a wild card, you say are you spec 13 brand TLD? Yes. You can only point this at a service and this obviously requires compliance. But before you can have this put in in the same way it's currently prohibited contract.

DANIELLE RUTHERFORD All righty. First in the queue, we have Steve Crocker and then Maarten.

STEVE CROCKER Great. Thank you. This is pretty interesting. I had not paid attention before, although the site finder in 2003 comes vividly back in memory. The criterion that you're proposing is that, there would not be multiple registrations. This is sort of a sales issue, a business issue that is being encoded into the rule here. I mean, that's the basis of the distinction that you're making.

I don't have a strong opinion one way or the other, but I want to play it back with sort of two pointers. The idea that if it's a brand TLD, then it does not go to have a bunch of competing registrations underneath it. But the same issue also applies downward when

you have second level domains that are registries like co.uk is a registry.

Now that's not a contracted party. I'll come to that in a second. But the basic idea that you're talking about is not specific to the top level, as I say, can be driven down as well. And so then the other aspect is that co.uk is not contracted party. Why isn't this a principle that applies across the entire spectrum, not just to contract it, not just to the gTLDs. And if the answer is, well, that's all we can control, please leave the room.

WARREN KUMARI There have actually been a number of ccTLDs that have had wildcards in them. Generally, these have been removed over time because they caused weird odd security issues. I believe co.uk doesn't allow wildcards specifically for the reason that there are multiple registrants with them. However, ICANN can't really control that because --

STEVE CROCKER Yeah. And my point about that is that we're now talking about something that has a combination of engineering and business issues and for the engineering issues the right form, it would seem to me is the IETF. But for the business issues, we don't have a working arrangement in which sensible business ideas are discussable across the entire spectrum, despite the fact that they should be.

WARREN KUMARI I mean, the DNS, I don't really know if it is a IETF thing because the DNS doesn't know that co.uk is different to reddit.com. And so, we can have advice that if you run a domain that there are multiple registrants in basically public.

STEVE CROCKER Exactly. So, this bumps into the fact that the notion of a registry is not, not cleanly encoded at the DNS level despite our colleague Jonathan's best efforts at being helpful in that area.

WARREN KUMARI The IETF has had multiple swings at this, right? We had the debound working part, Working Group we've had. I don't remember what there was before. There've been multiple attempts to try and actually put in the DNS.

BARRY LEIBA I think it's just multiple iterations of debound.

WARREN KUMARI Debound. Yeah, with different names. How does debound and debound two or something?

BARRY LEIBA Something like that.

WARREN KUMARI Yeah.

STEVE CROCKER I see in the chat, Danny McPherson says it's more complicated than you think, but I'm eager to hear what he has to say about that. Maarten?

MAARTEN AERTSEN Warren, Gautam, thank you for being so clear that the motivation for this is not security, stability, or resilience, and that you're bringing it to SSAC, even though you also wear an SSAC hat. So, I really appreciate that. Thank you.

WARREN KUMARI Yeah. I mean, it's entirely driven by let's make URLs look nicer.

STEVE CROCKER If I might. Just the comment that it's not a security stability issue, let me just take mild issue. It is in the sense that it's because of a security stability issue that the rule has been imposed. And so that's an overreach. I mean, the claim then is that that's a too broad a rule.

And since it came out of the security stability environment here, I would argue that it's just as much a security stability issue not so

much in preventing bad things from happening, but preventing good things from happening because of overreach.

MAARTEN AERTSEN: Sure. You can see it that way, but what I meant to say, and maybe I should have is I don't think as a committee, we are in the habit of bringing up business or other ideas ourselves because that's not our role. Right. And I think being clear that this is not an SSAC idea, but it's an idea from people that are also in SSAC to revisit or discuss blocking advice, as you've just nicely put. And I agree from that angle, you can say it is a security, but is clear what I was saying?

STEVE CROCKER: And well, to me, it's clear, but I would still take issue that I think our responsibility is, is neutral and is two-sided that if somebody comes to us --

BARRY LEIBA: Let's leave it at that. We're kind of drifting.

DANIELLE RUTHERFORD: Right. Next in the queue, we have Rick Wilhelm.

RICK WILHELM: Thanks. So, I'm highly skeptical of this approach because I think that there are limited considerations for how this is going to be gamed. And I think that when I see this is that if we add this

capability to a brand TLD, I think that a lot of people are going to be applying for brand and I'm here, I turn it into a quote, brand TLD that are really not brands, but they're going to fashion themselves as a brand in order to lever this thing.

So, they can have what I would then call pseudo registrations and give people space in the namespace, which is not a registration, but it's functionally equivalent to a registration because it starts to quack like a duck.

BARRY LEIBA Remind me what work party you chair.

RICK WILHELM Oh, RIDE. And so, this sort of sits in between RIDE's remit and the regular DNS. So, this sort of starts to blur the line inside of the standard DNS. So I think that we're going to have a lot of things that quack and swim and look like ducks, even though they're not paying registration fees and have registration data and have obligations like actual registration ducks do.

WARREN KUMARI So, yeah, I mean, I think that's what point two is designed to protect against. And the tricky bit as explaining the service part for the abuse side, I think the same thing currently, if somebody puts an abusive video on YouTube, it's YouTube's responsibility to deal with that.

So, if there's abusive content within one of these, it would be the brand operator's requirement to deal with it. But yeah, it would clearly be how exactly you define point two to ensure that this doesn't turn into a normal TLD, but without registrations.

RICK WILHELM

Sure. But what's interesting to me is that actually just about within the last week, I was cruising Reddit. I know you find that surprising, Jonathan, but I was, I saw a picture of YouTube from about 10 years ago and I saw a picture of YouTube today and the level of sophistication of the service is obviously grown because there are people at the Google that work on that.

And so, to say that, and we'll pick on Veritasium cause that's both a cool channel and the subject at hand to say that veritasium.youtube.com or youtube.com/Veritasium is not going to be further customizable and capable in the future to function basically as a website for the folks that work behind it is silly, right? It's going to get better and more capable and more customizable in the future because that's the evolution of technology.

WARREN KUMARI

I think that if it were to happen, ideally, ICANN Compliance would have teeth and would say your thing now looks too much like a web service.

RICK WILHELM: But the genies, the horses down the road, the genies out of the bottle, the two spaces out of the tube, the bells echoing off the village walls, you know, pick your metaphor, but it's too late at that point because it's not just .youtube.com that's out of the thing, but ICANN has given brand TLDs to all of these people up on the board and they can't undo that. And so, anyway, I realized that we've got a queue.

BARRY LEIBA: My hovercraft is full of eels. Please go to the second question.

RICK WILHELM: And I'm also, I'm highly curious as to who at ICANN said that was okay. And if they'd be willing to go on the record at that.

WARREN KUMARI: I don't know. I don't want to put words in their mouth.

BARRY LEIBA: Chat during the break so we can get to the other three questions.

DANIELLE RUTHERFORD: All right. Just a reminder that a priority goes to SSAC members for questions first. So, if you are not an SSAC member and you've got your hand raised, we may not get to you in the time remaining. And I've put the email address for SSAC support staff in the chat. If you

want to reach out to me and we'll connect you with the speakers. Next is Rod.

BARRY LEIBA Please keep your questions quick and your answers quicker.

DANIELLE RUTHERFORD Rod, go ahead.

ROD RASMUSSEN So, great. Hey, so this is how I got involved in the internet 30 plus years ago was actually figuring out that you could wildcard subdomains and do cool stuff with them. I also found that once you did that, things broke a little bit and that actually putting the actual entry into the DNS made it much, much better. And I think that especially with email, which is where I got into this, it would work better.

I'm a little, I do like this. I've heard this bantered about quite a bit. And I've always been of the mind that if you get a brand and you're using it just for your own stuff, it would be really useful to wildcard. So, I can stand up infrastructure, move it around, do whatever the heck I want to. And I don't have to worry about doing things with a registry. I can just stand it up in my own DNS, get things working, especially when you've got cloud computing and things like that, where you have things that may be ephemeral.

So that I think would be something to explore here is that side of things. This is the first time I've seen it tied to a service, which makes me less dubious than I was before on this, because I thought before it was just a way of getting out of the way from having to pay ICANN fees. Because I'm very concerned about users that are not the brand being responsible for part of the DNS.

Now tying it to service, that's really interesting. I'd like to dig into that a bit more, but there has been in the chat, there's a lot of dragons there to slay. But I do like to at least banter about the concept, but I also like the concept of doing that for using it for your brand internally. Thank you.

JOHN LEVINE I'll try to summarize stuff. If everybody were nice and smart, I think this would be a reasonable idea, but I do not believe that everybody is nice and smart. I believe this will be gamed. I do not believe that ICANN compliance has the technical or political skill to enforce this. So, I don't think we should do it.

BARRY LEIBA Okay. More to discuss during the break. Peter.

PETER THOMASSEN It's just a comment. So, one of the names that you list, at least one is in the public suffix list and has a wildcard, which is githubusercontent.com. It's obviously not subject to registry

agreements, but it's a similar case. So, that's something I haven't considered just to raise it.

And the second thing, can a TLD operator put a D name because that has the same effect, but doesn't require a wildcard on the second level? I'm not asking for you to answer that, but…

WARREN KUMARI: I don't know. I do want to note that Francisco has his hand up and maybe we should let him, he's not an SSAC person, but he might be commenting on --

BARRY LEIBA: We really are out of time. So, let's take this offline. Thank you. It was an interesting discussion. Thank you, everybody who presented. Thank you, everybody who came.

KATHY SCHNITT: Please stop the recording.

[END OF TRANSCRIPTION]