ICANN86 Seville | PF – Joint Session: NCSG and SSAC
Wednesday, June 10, 2026 – 10:00 to 11:15 CEST

ANDREA GLANDON

Hello and welcome to the joint session of the NCSG and SSAC. Please note that this session is being recorded and is governed by the ICANN Expected Standards of Behavior, the ICANN Community Anti-Harassment Policy, and the ICANN Community Participant Code of Conduct Concerning Statements of Interest.

Please observe the following guidelines to participate in this session. I will also post them in the chat for your reference. Only questions posted in the Zoom chat identified as a question will be read aloud during this session as time permits and when directed by the chair of this session. If you wish to speak, please raise your hand in Zoom or as otherwise directed. When speaking, please state your name for the record and speak clearly at a moderate pace. I will now hand the floor over to Rafik and Ram. You may begin.

RAFIK DAMAK

Thanks, Andrea, and thanks, everyone, for joining today for this joint meeting between the SSAC and the NCSG. So just maybe to say a few words, we are happy to have this regular interaction with the SSAC to share some points of view and also to learn more about the activity of the SSAC and see where there are some synergies

where we can cooperate and collaborate. And I think today it will be a good example on how those kind of interactions can be valuable for both sides. And with that, I will pass to Ram, if you want to add a few words.

RAM MOHAN

Thank you, good morning, buenos dias, and I am really pleased to be here with all of you. And the SSAC is pleased to be here with all of you. It's actually the second or the third time that we are meeting together and we are kind of still figuring out how this works out in a way that is good for both NCSG and for SSAC.

So I think from the SSAC's point of view today especially, we are here to learn because last year when we were speaking, I believe it was at the Prague meeting when we met and you were sharing with us about human rights and what a human rights assessment framework might be. And for me, just speaking personally, that was a new thing. That was something where I was like, oh, that's interesting. So I am here to learn. I think we are all here from the SSAC to learn.

And Rafik, perhaps one thing that might be useful just because of the relative youth of our interactions, perhaps we just take a moment and introduce, just go around and just have people introduce themselves, particularly SSAC members from my side. I would like for them to just share not just their name but their affiliation and kind of what they have been doing in the SSAC that

might be of value and perhaps you could do the same from the NCSG side. What do you think about that as a starter?

Okay, great. So then let me start with folks on my right and ask for SSAC members to take the microphone and just introduce themselves, but also share a little bit about their interests and what they do in their day jobs.

GEORGIA OSBORN I'm Georgia Osborn, hello. I work in my day job and in the UK regulator Ofcom as part of online safety tech.

JOHN LEVINE I'm John Levine. I guess I'm an independent ex-academic. I've been doing a lot of standard stuff and recently I've spun up a new little training foundation where we're attempting to do cyber security education in developing countries.

VASYL "BILLY" BRATCHENKO Hi, I'm Vasyl Bratchenko from Namecheap. I lead anti-abuse and risk management teams in Namecheap.

RAFFAELE SOMMESE I'm Raffaele Sommese from the University of Twente, a member of SSAC. I'm an assistant professor at the university. I do a lot of research in the DNS area and security and stability of the DNS.

TAPANI TARVAINEN

I'm Tapani Tarvainen for NCSG, and I'm GNSO councilor at the moment. My name suggests I represent Electronic Frontier Finland, not the foundation, mind you, but I'm actually already retired. This is just an unpaid position here. My background is very much of a techie at a long university career and I'm actually, perhaps, understand even as much about security issues than the policy issues that I'm supposed to be working here. I was very interested in the DNS session, for example, we had a few days back.

BARRY LEIBA

I'm Barry Leiba. My day job is to actually do internet standards work in the application and security layers, and I love that. I get paid to do volunteer work, is kind of what it is, and I'm also on the Internet Society Board of Trustees.

FARZANEH BADIEI

Hi, I'm Farzaneh Badiei. I'm a recovering academic. It's been five years, so I should stop saying that. I run Digital Medusa, which is an advisory that works on Human Rights Impact Assessment, as well as access to the internet at the infrastructure level, but also in social media and app governance. I'm a member of NCSG, the Non-Commercial Stakeholder Group, and on the GNSO Council.

RAM MOHAN

I'm Ram Mohan. I'm the Chair of the SSAC, but in my day job, I'm the Chief Strategy Officer for Identity Digital. It's a domain name registry company, but I also spend and have spent a lot of my time

in my career working on helping the internet become multilingual, internationalized domain names, universal acceptance, a lot of work in that area, as well as spend a lot of my time on the operational side of things, helping implement technologies like DNSSEC or anti-abuse systems on a global scale.

RAFIK DAMAK

I'm Rafik Damak, the current Chair of the Non-Commercial Stakeholder Group till the end of the Bali meeting. I was in the GNSO Council for several years, so that's how I was involved in ICANN representing NCSG, and for my day job, it has really nothing to do with DNS, but I work on the data center business.

TARA WHALEN

Hello, I'm Tara Whalen. I am the Vice Chair of SSAC. In my day job, I work at the World Wide Web Consortium, where I am privacy lead, so like a lot of you here, technical standards, open standards on the web, and trying to make everything as privacy-preserving as possible, and there's also a little bit of policy engagement work that started to come along with that.

JEFF BEDSER

Hi, I'm Jeff Bedser. I'm also with SSAC. In my day job, I'm the CEO of CleanDNS and spend all of our time mitigating online harms and DNS abuse.

SUZANNE WOOLF: I'm Suzanne Woolf, SSAC member. My day job is for the Public Interest Registry, PIR, and my job title has something to do with technical community engagement, which in the real world means standards and tech policy and all of the places, all the things that happen where policy crosses over with technology, and I'm spending a lot of time this week representing SSAC on the review of reviews CCG.

WARREN KUMARI: Hey, I'm Warren Kumari. I'm part of SSAC, day job as Google, where I do internet standards, and I also serve on the Internet Architecture Board.

WES HARDAKER: I'm Wes Hardaker. I'm an internet standards engineer trying to make the internet even better. I do a lot of security research. I'm a fairly new SSAC member. I'm the USC-ISI representative to the root server committee, and I'm the RSSAC liaison to the ICANN Board.

SHIVA BISSESSAR: Hi, Shiva Bissessar. I'm not an SSAC member. I applied yesterday. I'm an information security expert based in the Caribbean. I'm just here to learn. Thank you.

PETER THOMASSEN: Hello, I'm Peter Thomassen from deSEC, which is a not-for-profit that also tries to improve the internet, particularly by improving

	the situation of DNSSEC by making it easier to use, to make it automatic. On our platform at deSEC.io, you can see how that integrated DNSSEC hosting works. Essentially, you don't notice any of that. It's just easy. Within the ITF and ICANN space, I work on internet standards that standardize the automation for DNSSEC, and we're trying to get that deployed.
JAVIER	Javier [inaudible – 00:10:07]. We are working with TLDs and the root domain to keep it live. We will provide services for all of them. In my long life in the telcos space, we've been developing the internet from the major telcos within Spain and Europe.
RAM MOHAN	Thank you so much. I also want to recognize some folks who are online. Laurin Weissinger is also an SSAC member. Laurin, you're online, I think, so please speak up. Yes.
LAURIN WEISSINGER	Hi, everyone. I'm Laurin. I'm only remote for this session. I'll be back on site during the next break. I work on testing and evaluating AI systems and AI and security standards, mostly associated with the National Institute for Standards and Technology in the US. I teach security at Tufts and Berkeley in the time that is left over. Focusing on obviously AI, but also DNS firearms and DNS abuse.

RAM MOHAN Is there anyone else online who would like to speak up?

ANDREA GLANDON Ram, I'll just note that Julf Helsingius is also remote. His mic isn't working, but he's a GNSO councilor for NCSG.

RAM MOHAN Thanks, Andrea. I would be remiss in saying that if you look at SSAC and you look at how the SSAC works and why the SSAC is able to do so much of what it does, it's because we have the most amazing staff support. I'll just give a shout out to the folks who quietly sit in the back, but who actually make us look good. I'll pass the mic to you guys, just to introduce yourself briefly and let people know who you are. Have mics. Okay. There's Danielle Rutherford there in the back, and then Kathy Schnitt, and there's Dan Gluck. Anyone else from staff who's here? No.

ANDREA GLANDON I'm Andrea Glandon. I'm staff support for NCSG.

RAM MOHAN So, I mean, you're the unsung heroes, but we want to make sure that you get the recognition that you deserve.

FARZANEH BADIEI I sing for Andrea every day.

RAM MOHAN

Okay. Rafik, we're on to you now to inform us about what this means, Human Rights Impact Assessment framework.

RAFIK DAMAK

Thanks, Ram. This is a good example of follow-up of, as you said, or mentioned, the discussion we had in Prague when, at that time, we asked, how do you do in the SSAC when you are drafting your reports from human rights standpoints? And so, there was a request, those meetings, is to have kind of briefing explanation, so to build more awareness, and to explain how it can be relevant and work for you. So, for today, we asked Farzaneh Badiei to explain, to give a briefing about Human Rights Impact Assessment, and including some examples, some cases to be more concrete and see how that can be relevant for your case. And with that, I will ask Farzaneh to start.

FARZANEH BADIEI

Thank you, Rafik. So, I prepared some slides, but just that we are working on this Human Rights Impact Assessment framework. Nothing is set in stone. There are many experts around the world who are working on it and trying to improve it. There are many shortcomings that we need to address, as we are always reminded that the human rights values are sometimes conflicting, and it's not possible to uphold all of them at the same time. So, when should we do balancing? When does the benefit of a mechanism outweigh

its disadvantages? So, these are the issues that the Human Rights Impact Assessment tries to address.

And we came up with some slides. I'm going to go through what Human Rights Impact Assessment, how we do it at ICANN. And also, I'm going to tell you a little bit about the GNSO Council and what happened at the PDPs. But know that this is an iterative process. It's not like the mechanism is always evolving and trying to improve. So, if you have feedback, if you think that we are doing it wrong, let us know. Next slide.

So, during the IANA transition and the accountability work stream, we managed to have a kind of general clause in ICANN bylaws that says that ICANN should respect human rights as defined in international law. And it does not require ICANN to uphold them. So, it means that it is not, it doesn't mean that it's not enforceable, but these are guidelines that ICANN should consider. And then the GNSO Council, when they were implementing the human rights requirement, the GNSO Council decided to come up with a Human Rights Impact Assessment requirement for each PDP that they do. The PDP is the policy development process for the issues that GNSO Council tries to make policy about.

And now we did the first, when I say we did the first, I don't mean NCSG only. When we do the Human Rights Impact Assessments at GNSO Council, it's done by staff and the working group members. And the first one was on Latin diacritics, which is another issue that

has many human rights concerns, so it was pretty easy. The DNS abuse one is going to be fun.

So, what sorts of methods do we use in order to do Human Rights Impact Assessments in the human rights community and the digital rights community? We have one thing that is called the rapid Human Rights Impact Assessment method, which I quite like. You look at the decisions that you've made, the policies that you've set, and I'm going to go through the set of questions, and you ask these questions and try to answer. And if we get the time, I'm going to talk a little bit about how we can consider human rights in law enforcement authentication that we are discussing, and also associated domains. Next slide.

I went through all of this. So, we did something fun on a GAC communiqué, a few of the GAC communiqués. We did a Human Rights Impact Assessment on the advice, which I can give you one example of as well. So, a Human Rights Impact Assessment is kind of like prioritization of actual or potential adverse human rights impacts and making recommendations for appropriate actions to address those impacts. I know many of you do risk management, so a Human Rights Impact Assessment is also some kind of assessing the risk to human rights. We are not claiming that -- and we also look at the likelihood of the risk.

So, we apply this to GAC communiqués, to PDP proposals and policy amendments, and we can do it to SSAC advice too, if you want. But generally, what we do is identify the rights that are at

risk, whether it be freedom of expression, privacy, assembly, the right to assembly and association. And these rights are generally as they are stipulated in the UDHR and other internationally recognized human rights.

We also look at the affected communities, who is most affected in terms of human rights, their human rights with this policy. And also, we do stakeholder engagement, we talk to you, we also have these sessions. Almost every ICANN meeting, we have Human Rights Impact Assessment session that we talk to the community, we receive their feedback. And then, as a result of these processes, we provide some remedies and mitigation mechanism to address the risk. Next slide.

So, I keep saying this is like the rapid thing, because I just want to say that this is not like a multi-million dollar project that's going to take years. We do it succinctly, and also ICANN staff have been able to use the templates that were provided by the community and do Human Rights Impact Assessment in an efficient manner.

So, first, who is affected by this policy? And rights holders, unfortunately, these days, it's more about copyrights holders, and here by rights holders, we actually mean human rights. And so, who is affected? Is the registrant affected? Is the user who uses online services affected, potentially affected and at risk? What sort of community are they? Are they journalists, activists, minority groups? And what's the severity? Is the severity of harm and risk to human rights high? Is it unlawful arrest, imprisonment? Could

it lead to cruel punishment or not? And then, what are the longer-term implications, chain effect on domain names, free expression, incentivizes inaccurate data registration, and then erosion of trust.

And then also, we look at peer practice. How have other organizations that are similar to ICANN addressed these issues? Because we don't want to compare ICANN to industries that don't have similar mandate. So, for example, in one Human Rights Impact Assessment that we did, we saw that there should be some kind of transparency in this reporting system of RDRS. I don't know if you all know what RDRS is, but it receives the request for private, sensitive information of domain name registrant and sends it to the registrar.

So, we wanted to see if they can have some transparency reporting on law enforcement and others, like how many requests were there, which jurisdiction they were based in. And we looked at other reports, and we saw that RIPE NCC does similar reports and use that as the justification and the basis of our suggestion. And then, what's the mitigation? What are the remedies? What can we do to reduce the risk, if we can do anything? Next slide.

And if I'm going on and on, just stop me, and we can have a conversation. I hope this is useful. I just wanted to give you an example of a Human Rights Impact Assessment that we did on GAC Communiqué, that they asked for the confidentiality of law enforcement requests. We did a Human Rights Impact Assessment, and we came to the conclusion that absolute confidentiality might

actually put human rights at risk. So, we asked for and advocated for more transparency. And, of course, it can be confidential. But, for example, you can have, like, after six months of the investigation has passed, you can report on it, or you can report on it at the aggregate high-level level, high-level system. So, that's about it. We can go to --

RAM MOHAN I have a question on this. So, the conclusion says that ICANN should not grant law enforcement the option to seek disclosure confidentially, right?

FARZANEH BADIEI Yes. So that's the absolute term, but as I said, I fixed it. So, basically, it should not grant law enforcement the option to seek disclosure confidentially, but it is possible to come up with ways that after six months, they can report on it. So, this is, like, they should not be able to obfuscate and cover up their identity when they ask for information, when they submit the request.

RAM MOHAN But what about legitimate cases where they actually do need to hold the information confidential, where they are involved in a takedown of a system, and they are going after not just one criminal, but they're going after an entire criminal network? I mean we work with organizations that do that. How would this work on a situation like that? You had a question.

FARZANEH BADIEI

Sorry to tell you Ram. We actually worked with Gabriel from FBI on this, and we came up with a way for our DRS to provide some sort of transparency, but at the same time, not to jeopardize the investigation. So, you don't need absolute confidentiality for doing that. And when we say confidentiality, when we say transparency, we don't mean that, like, you have to, like, tell us what the investigation is about and all sorts of things. We just mean that, like, there has to be, like, aggregate data and saying that, like, you requested this. We prefer to have the purpose of the request, but if that's not possible to disclose it now, it can be done later.

RAM MOHAN

I saw Wes's hand up, and I saw John's hand up. So, Wes, to you first.

WES HARDAKER

Yeah, thanks very much, Ram. And I'm very appreciative of this work, having done a decent amount of research, produced a fairly lengthy report dealing with the types of malicious activity that tends to be published online can be quite severe. And the problem is that there's tension between people that might be harmed because they're posting completely legitimate information that might be disparaging to their government or systems versus information that might be published that is causing actual harm to somebody else. And so, malicious actors tend to be very good at

finding locations where they can publish content that is very hard to take down, if you look into bulletproof hosting or things like that.

So, it's unclear, a decent path forward that provides both the rights mitigations on both sides for the content that's being published that's malicious versus somebody being persecuted for information that should be a free form of communication. I don't have a good answer to that, but the problem is that lengthy delays of such analysis actually will cause a problem in themselves, possibly harming the information that was published that really shouldn't be online. So, I'd love to hear a solution to that, but I don't think it's quick in coming.

JOHN LEVINE

Yeah, I'm going to pile on a little bit. I have to say that I find this analysis deeply disappointing because the academic community, at least as represented here, has spent years thinking only about Article 18. But of course, there are 35 other articles, meaning like Article 12 about attacks on honor, which is basically what he's talking about, or Article 17, which is about having your stuff stolen, you know.

And we spend way too much time working with law enforcement and with private organizations that are attempting to understand and address these online evils. And honestly, in analyses like this, I see no evidence at all that you're even thinking about the possibility that the cops might actually have a job to do, you know. And so I would emphasize even more than Wes did, like, if you want

to be credible and you want to be useful, I mean, you need to -- The reason there's 35 articles is because they're all in tension with each other and just saying more free speech simply ignores all the other issues.

And I would, actually, I would direct your attention yesterday at the NextGen. There was a really excellent talk by a young man from the University College London, where he was, like, attempting to look at the balance of the WHOIS disclosure information the current scheme is totally screwed up. And he had a very good analysis of, here's why it makes sense to keep some stuff private, whereas here why it's like, if you have an active investigation waiting a week to get an answer basically just destroys the investigation.

I mean, so I really hope that you'll go back and look at the whole thing and look for some more balance, because although these are issues are important, they're not the only issues. There's other stuff that's just as important.

FARZANEH BADIEI

This was just an example about, of course, when we do impact assessment, we do the balancing. So the impact assessment method has the balancing in it. And as a community, this is why we have to talk to other communities to understand how their work is affected. This is why we have to talk to the law enforcement and tell them, okay, so why do we need confidentiality? And how can we provide some sort of transparency while not jeopardizing your investigation? But your point is taken, and you have been making

this point for the past 15 years, and it's very valid. And we are working on it. And I hope that next time we present something that is credible to you. Yeah.

ANDREW CAMPLING

Hi, Andrew Campling, an observer, so not part of either body. Just really agreeing to the point that John and Wes made on balance, and perhaps to add some color to that, because we do tend to, in my view, completely over-fixate on the privacy rights and other rights of registrants. Yes, they're important. We rarely, in the discussions, for example, in the GAC yesterday on RDRS, there was absolutely no discussion about the rights of victims or potential victims.

And to put some color on that, last year, online, so tech facilitated online fraud, $442 billion worth. I think it's about a quarter of adults around the world are victims of scams last year. Or children, roughly 10% of children are victims of online sexual exploitation. So this is all tech facilitated. You know, domains are the root of that. So when we obfuscate registration data, when we fixate on the rights, privacy rights of registrants, we completely lose the voice of victims. And any delay, as John just said, extends the scale of harm. And we move away from things like qualified privacy rights into absolute right to life. So we have to do proper balancing assessments, not just a one-sided, fairly superficial assessment.

FARZANEH BADIEI

Absolutely. It's about balancing. And I'm not talking about my own opinion here. I'm talking about ICANN. I might have my own personal opinions. But at the moment, at ICANN, what we do in terms of Human Rights Impact Assessment, balancing legitimate interest is a part and parcel of the Human Rights Impact Assessment. And of course, as you know, we have all these sessions. And this is why we also have human rights town hall. Kind of like sometimes we have these sessions that people come in and they say that these are the human rights that you are not considering. And so we want to consider those and then see how we can do the balancing.

Can we go to the next one? Okay, this is Wes's favorite topic, authentication and authorization. I thought it was a good case study because you also have it as a topic, as an agenda item to discuss, right? So let me tell you a little bit about our opinion on this. We have not yet formulated an opinion that we can put forward. So whatever you are hearing here is draft. But we have certain concerns with the authentication authorization that is happening and the conversation that is happening at SSAD and the urgent requests. So would you like me to just go through our concerns and then we can open up? Next slide, Andrew.

Yeah, absolutely. Yes. So some of the things that we want to bring to the attention of the community is that authentication is hard and these systems can get hacked, especially when it comes to law enforcement. And sometimes unforged emergency requests have been done before that the system got hacked. And as a result of

the hack in the system, it was authentication system for the law enforcement. So the hackers pretended that they're law enforcement. And in some cases, the data was disclosed to them, to the hackers, because it was an emergency request.

So the risk here is real. We are not hypothesizing. There was like Google LERS portal that got hacked in 2024. And that did not result in disclosure of private data. But there was another case that when it got hacked, there were like reputable, big resourceful companies involved, but they still disclosed the data. So that's one of our concerns with the authentication system. What if it gets hacked? So we want to see good security measures for whatever authentication mechanism that we come up with at ICANN. And I think that SSAC is very well placed to give advice on how to come up with it, right?

RAM MOHAN

I'm scratching my head, literally, because I look at that and I say, that's kind of a basic standard thing, right? To say, protect your credentials and build systems that are effective in detecting when credential compromise happens, right? But we don't look at it from a, oh, that has an impact necessarily on human rights. We look at it as it's an appropriate security measure to make sure that if there are forged credentials, that there are mechanisms inside of organizations to detect such forgeries and then to take quick mitigation steps on it, right?

So if you were to write an advisory that says, authentication of emergency pathways that skip judicial oversight are structurally vulnerable to abuse, I think inside of the SSAC, I'm speaking for myself, inside of the SSAC, I think I'd have members saying, duh, that's like obvious, right? So should we be saying things like that? Because that's normally not what we say.

FARZANEH BADIEI: But that's not what we are asking. What we are saying is to contribute to make the system secure, just to add voice on that.

WARREN KUMARI: I mean, seeing as you mentioned RIPE earlier, it's possibly useful to sort of draw a correlation here to some of the networking practices. It used to be very common that the way somebody would join a network and be allowed to announce a set of network stuff was by sending a letter of authorization, which is basically like, here's a piece of paper with random letterhead saying, I am good, please authorize me with a random signature.

That's kind of similar to what we're getting here, right? A registry or registrar gets a random piece of paper with some icon that kind of maybe kind of sort of looks like it's an official stamp and they have to be like, that seems reasonable. Instead, if we had an actual authentication system where law enforcement could prove that they have been authorized and credentialed in some sort of useful manner, and the background information behind that, you've now

moved from a, somebody has to look at a piece of paper and try and infer if this is the correct police icon from Uzbekistan, to here is a system that shows that this person is actually the legitimate person. They've been credentialed by Uzbekistan.

They are part of a police system and it's a fully enclosed system where you can get information about what they're requesting. You now have moved from, somebody has to guess to, we have a system that can authenticate and provide. So the way I'm hearing you say, like I've lost my, like grown a second head.

RAM MOHAN What I'm hearing you say, just to paraphrase is you had to move from assertion of authority to validation of authority.

WARREN KUMARI And sort of the reason I started off mentioning RIPE and the routing system is we've moved from random letters of authorization to the RPKI where there is an automated and secure manner to verify this attestation was made with the required crypto stuff and a key proving that the person asking for it is actually the real person and is authorized.

RAM MOHAN Got it. Okay. There's Barry and then Wes.

BARRY LEIBA

So there's some work going on in the IETF called Digital Emblems, and that was, it's intended as visual things that are also scannable, digitally secured so that you can identify legitimate hospitals and Red Cross people and that sort of thing that could also be used to identify law enforcement, legitimate law enforcement.

But be careful what you're asking for, because SSAC is more likely to say we need to balance the needs of the two of law enforcement and human rights people. I don't hear that. I hear extremism, and be careful about that. A few instances of something going wrong doesn't mean the entire system is wrong. We need to look at the system and see what the right balance is. And that's likely to be what SSAC says if we say anything.

FARZANEH BADIEI

So we want an authentication mechanism. It is for human rights sake. An authenticated request is that the registrar can actually verify that this is good for human rights. What we are asking is when you come up with an authentication system, it would be great if you do it securely, like come up with the security measures, so that the likelihood of getting hacked would be less, would be lowered. Because when it gets hacked, then it will put the registrant at risk. I'm sorry that you're hearing some extremism. It must be my radical views that give that air.

BARRY LEIBA

To be fair, it's also hard to hear anything in this room.

FARZANEH BADIEI

I'm sorry about that. We actually insisted during the EPDP on the accreditation, and our privacy protection people want authentication. Let's make that very clear. I think Wes wants to make a very good point of authorization. No. So if you're not going to make it, Wes, I'm going to make it. But authentication and authorization are two separate processes at ICANN, and we can go through that on the next slide. But it doesn't mean that if the authentication system gets hacked, it doesn't mean that the registrar necessarily would disclose the data.

BARRY LEIBA

I don't think you're going to hear any argument against that.

WES HARDAKER

Yeah, thanks. I think one of the hardest things that people believe is that security can solve all problems, and it can't. Unfortunately, as much as we would like a hack-proof authentication system, they don't exist. Security people love to say, I've created a key that is beyond the lifetime of the universe that you can't crack it, unless it's stolen.

And we have levels of security that we add to protecting keys. The keys that protect the top of the DNS tree for DNSSEC are very well encapsulated in physical security processes that are handled very carefully, and there's a huge cost associated with that. And it

always comes down to a trade-off of how much you're willing to pay for the level of anti-hacking that you can put forward.

The one thing to always remember in those situations is that adding some security is always better than having no security. So even the worst authentication system actually improves, which is getting back to Warren's point earlier of a digital authentication system is better than letterhead, which has no security. We keep making improvements. So we do have to be careful. You can't get to a hack-proof authentication system. They don't exist. You can make them better and better, however.

RAM MOHAN

So I think, at least the way I'm hearing it is, perhaps there is the middle ground that you want us to get to, but we have to hear it in a way that we can actually engage. If Barry is saying he's hearing it as in one end of the spectrum, then we had to think about, and maybe to make the case, the NCSG has had to go to the end of the spectrum because you're sometimes not heard, but that's not what you'll see with the SSAC. I think you'll see us really willing to engage, but we need to also hear about how do we get it to that middle ground, where we tend to be much more in the middle of these things. So just my observations.

FARZANEH BADIEI

We are not in the middle. We agree. We need authentication. We need authentication. There is no, like, we are not challenging. We

are not saying we should not have authentication. As I said, we have been advocating for authentication and accreditation the past 10 years.

So all we are saying is that if the system gets hacked, there are going to be consequences. So we should have policy and technical measures in order to reduce the risk. And also, like, we are not talking in, like, we are not saying we should not affect human rights at all. We should just reduce the risk. That's why we do risk analysis. Should we go to the -- is there any--?

ANDREA GLANDON There are a couple of hands up.

ANDREW CAMPLING Yeah, sorry. Andrew Campling, again, referring to the RDRS discussion yesterday at GAC. There's already a system that Interpol uses for authentication. I know the US law enforcement agencies use one, and I think they're trying to at least discuss whether they should converge on some sort of standardized way within the law enforcement agencies. In other words, I think this is a problem to be solved there rather than an Internet standards problem, because I think solving it here is fraught with difficulties to validate if someone is a member of a police force. I can't see that being a protocol-type problem.

RAM MOHAN Wes has a two-finger to that. Sorry, Warren has a two-finger to that.

WARREN KUMARI No, I've got more of a longer comment, so I'll wait till I bump into you.

RAM MOHAN Well, you're next in the queue anyway.

WARREN KUMARI I don't think NCSG is on the extremism side of this. I think we're just talking past each other. If we build an authorization system, it will get hacked at some point, and some set of people will lose their credentials. There's also just because somebody happens to be law enforcement in some jurisdiction, doesn't mean that they should automatically get access to everything. I think that whatever system gets created, it shouldn't be, I am law enforcement, here's my badge, tell me all the stuff.

The system needs to be able to provide enough metadata about the request, so when somebody shows up and says, I am law enforcement, I am part of the United States Park Service Police, that is a very different meaning to, I am law enforcement, I am part of U. S. Secret Service, or I am part of Uzbekistan's local police force, or I am Interpol. There's very different sets of information wrapped up in what that is, and what their rights, and what their jurisdiction is.

Saying things like, the FBI/U.S. government and Interpol have authentication systems. They do, but it says, I am member of group, not, I am member of group, this is my type of credential, I happen to work in cybercrime, this is the jurisdiction I am responsible for. Instead, you get a yes, no answer. You get basically authorization, not authorization and metadata. If a registry or registrar gets this, they have no way of knowing what the actual authorization is for. They see, I have a badge, not, I have this sort of shape, and this sort of stuff that I work on, and I am trusted at this level.

The janitor at the FBI is presumably very different to, we'll use Gabriel as an example, they do very different things, they have very different sets of knowledge and rights. Some set of people who are accredited law enforcement aren't necessarily people that a registry or registrar would be comfortable sharing information with, which is why most or many registries require a court order to release stuff, not just, this person has a badge, therefore, and so the system should also be able to do stuff like, I am this sort of person, this is why I care, here is information about the court order that I have related to this, and instead, we seem to be talking about person is police, therefore, not person is police and has this backup information showing why they have any standing to ask it.

RAM MOHAN Thanks, Warren. There's a two-finger here, and then I'll come to you.

BARRY LEIBA

In addition to what Warren says, it's not just about identifying which law enforcement you are, but also ensuring that the system as a whole has checks and balances, and for instance, just because you're law enforcement, you also need to authenticate that a warrant was issued and that sort of thing, and then what kind, maybe you and I probably agree that FISA warrants kind of suck, so yeah.

TAPANI TARVAINEN

Tapani Tarvainen, for the record. I just have to defend paperwork a little, because these, in and of themselves, easily-forgable paper letters have one advantage or disadvantage, depending on how you view it, because they don't scale. Forging one letter is easy, but if you want to get a million of them, it's hard, whereas if you break a central system and hack it thoroughly, you get all the million at once, so it's not quite that simple, and the point here being that if we have a centralized system, the more centralized, standardized, whatever, the more you gain by breaking it at once.

RAM MOHAN

Okay, so Farzaneh, where do you want to take the rest of the conversation, because we have like 20 minutes.

FARZANEH BADIEI

Twenty minutes, that's plenty of time.

RAM MOHAN Okay, then we'll go back to you.

FARZANEH BADIEI So, I made this example because we are having a conversation, actually, at SSAC, and Steve Crocker, who is a member of SSAC, is making incredible comments that we agree with on authentication, and one of his points was that authentication is supposed to generate that kind of trust in the registrar to put all of this evidence together, and also, at the authorization level, get the submission form and see why they want this data, and then make an accurate decision.

So, this is all to help the registrar and the registry to do this, and also do a fundamental rights balancing. And that's another thing that he had a question about, like, how do we do fundamental rights balancing that I wanted to go through. I don't know if we get the time. And some of the elements, the data elements that Warren mentioned here, I think we need to think about it in the authentication mechanism.

I don't know if at the moment the group just wants something basic, just like the system should say who is behind, if the person who's claiming that they are law enforcement, they are law enforcement or not. So that's it, that's what they want to have, yeah. And we believe that it should do more than that, but there is authorization, there is a second step, which is authorization.

So after you get authenticated and you are in the system, you can submit a request for disclosure of data. In that form then you provide the reason and why you need this, and if there is any kind of like a warrant or anything, you just like upload it, and like the emphasis is that they say that this is the stage of authorization, which is the assessment of the request, and then disclosing the data is the more important one, and authentication might not be, like, authentication can be like some kind of like a basic process, which I don't personally agree with. I think that when you authenticate an organization or law enforcement agency, you give them a little bit of credibility, and to do the authentication, I think you should do more than just making sure that you are the law enforcement from Uzbekistan.

So this is like an ongoing conversation, and we will come back to you with our analysis on authentication, see what you think, and yeah, we can follow up on the conversation. Rafik, shall I just go on? So there is an authorization case study as well, if you want me to go through it.

RAFIK DAMAK Okay, so, I think about the time, because there are next agendas more about follow up on some action items.

FARZANEH BADIEI Yeah.

RAFIK DAMAK

I'm not sure it will take that much time, maybe. Yeah, so, should be okay.

FARZANEH BADIEI

Yeah, okay, so, let's go to the next slide. No, let's go to the next slide, Andrea, yeah, because I'm going to get roasted. Okay, so, for authorization, so, what we want in authorization, so, this authorization is when the law enforcement is authenticated, and then they submit the form to get access to the registrant date.

What we want to see in this form, we want to enable the registrar or the registry to verify the legitimacy, is the purpose legitimate, the necessity, is this the least invasive means of resolving this issue, and then proportionality, is all the data that they want are proportionate to the aim. And then, for example, when registrar or registry gets a request from law enforcement agencies, and they should do fundamental rights balancing, and at NCSG, we are not saying that this fundamental rights balancing should be a contractual obligation.

We would like it to be, but at the moment, it's just like a best practice. But in order to do that kind of fundamental rights balancing, and balancing the legitimate interest, the registrar should consider whether there is active conflict or crisis in the requesting country, ongoing conflict or suspension of rule of law changes, there are calculus changes there, and then sensitive or a vulnerable registrant, is the registrant like an activist or a journalist,

and country freedom ranking in general, and was the judicial authorization provided, was it a subpoena, was it a warrant.

And so these are like the things that the registrars can consider in order to -- and this is like a bit of a Human Rights Impact Assessment is here, like, you look at legitimacy, necessity, and proportionality, and consider the situation of the registrants as well.

RAM MOHAN Let me just ask Vasyl, if you can speak to at say Namecheap as an example, what is the process that you go through when you get requests for these kinds of access?

VASYL "BILLY" BRATCHENKO We actually escalate this to our legal team who are specialized on that, because it takes a lot of training and expertise to figure out whether this person is an activist or a terrorist. It's a tricky thing in some countries, so that's why we actually have a dedicated team which is outside of my control.

FARZANEH BADIEI Yeah, so I just wanted to make an example like what we are asking for, because this also like goes back to your point, Warren, that like just because it's from this law enforcement agency, the request is from this certain law enforcement agency doesn't mean that the registrar should hand in, like they should like do these, like they should look at the request and see whether it's legitimate,

necessary, and proportionate, and so this is like our position at the moment at SSAC. All right, let's go to the next slide.

WARREN KUMARI

I mean, just a sort of a very quick thing, I'll note that escalating this to your legal department has significant costs and you have significant costs dealing with it, blah, blah, blah. I think that one of the risks with having a centralized system or any authentication system is it becomes incredibly easy to move from let's take this and check with our legal team and blah, blah, blah, to the system said this person's law enforcement, so therefore we'll just give it to them, right? Seems like that's very quickly going to get automated. Person presented something, if there is any legal risk, well, the credentialized system said that they're allowed, so they must be good. Like it's a slippery slope concern, I think.

FARZANEH BADIEI

Yes, that's a very good point. So should we go to the next? Okay, and so we just wanted to also like tell you a little bit about our DNS abuse mitigation and associated domain check opinions, and we are worried about this, the implications that this method could have on the domain name registrant and privacy, and also if it could lead potentially to over removal and over suspension of the domain names.

Now, one thing is that we have to do a data protection impact assessment on the associated domain checks, and we wanted to

know if there are any technical privacy concerns when it comes to associated domain check. Like amongst SSAC, are you worried about this? Do you think that it could potentially have an impact on data protection and privacy? What can be done about it?

RAM MOHAN

We have a couple of SSAC members who are directly part of that PDP. What I've heard so far is that there is good progress in this area. We recognize that sometimes the associated domain check results in identifying a name or a series of names that may actually not be associated with abuse. They may be registered for some other reason, and so there is a false positive issue to think about and to work through.

But my sense of it is that in the normal case, there is support for working strongly with associated domain checks because we see in real practice that bad actors are utilizing the loophole in the current system where the delay in investigation of one name means that you just register another 10,000 names, and you run the table on all of those, and you cause real harm. So there's an asymmetry there, which I think the associated domain checks, if it's done the way we think it should be done, will reduce that asymmetry, will bring back a much more rapid way of looking at it.

Inside the SSAC, we've not had a lot of discussion on, especially with the increased velocity and scale of attacks, whether these associated domain checks, the associated domains, whether action should be taken on them preemptively or whether action

should be taken on them retrospectively. And so we have not come to a conclusion on that internally, but several of us who are operators have a particular point of view on, if you see something bad and there's other stuff from the same bad actor, there's a likelihood that all the rest might also be bad. But I don't know that we have come to a conclusion on that. Vasyl.

VASYL "BILLY" BRATCHENKO Just my personal opinion. I would say that there is no risk to privacy, like additional risk, because we operate with the same amount of data as we would do without the associated domain check. So it's more about risk of taking down over suspension and so on. That's true. This is possible. But in terms of privacy, personally, I don't see additional risks.

FARZANEH BADIEI Yeah, great. We are just asking experts whether they see additional risk. But also, we are very clear in the working group that the registrar should work with available data and not to collect additional data for this. So that could also be a safeguard. Just one second. Another thing that we are not very clear is what is associated domain check. There is no spec about it. Where does it start and where does it end? And what does it entail? So what sort of actions are taken in order to do associated domain check? Is there any technical document that lays this out?

RAM MOHAN I have not seen one. I mean, inside of my registry, we do this, and we have our own internal definition for it. I know several other colleagues in the industry who do similar things. But I have not seen kind of an industry-wide uniform definition of this yet.

ANDREW CAMPLING Just on the associated domain checks, you have a point anyway, is that the registrar, say, if they are in the EU under GDPR, is perfectly entitled anyway to do that because they are entitled to prevent fraud on their systems. It almost certainly breaches their terms of service. So they feel like they are entitled to do it for their own reasons in any case. And there is certainly no additional privacy risk.

RAM MOHAN Yeah, I think, Andrew, my perspective is that they are entitled to do it does not mean they always do it. So I think it is important that we provide strong incentives and strong kind of drivers to encourage this ecosystem to clean up those places. Jeff?

JEFF BEDSER To follow up on Farzi's question, the way I normally see it is the industry relies on the initial report of the harm, and that that pivot or that associated check is usually based on whatever evidencing point was the key evidencing point to take that mitigative action against the harm. So if it happened to be a screenshot of a

particular phishing page, if they can find that same phishing page elsewhere, that might be how they do the pivot.

If it is the way the string is designed, like the words and characters or names within the string, that also can be the pivot. Sometimes it is all the ones at the exact same time that were registered, so it is temporal. But it is usually just based on that initial report, and they pivot to what other domains are related to that report that gives them that reason to check.

FARZANEH BADIEI

Yeah, so let us go to the last one. No, I like the name. Okay, so these are all the things that we have been doing on the tabletop exercises on Human Rights Impact Assessment and stuff, but I covered this. Let us go to the other.

Okay, so these are like some of the things that we are asking to consider. This is just a draft, but it would be great if we could work on authentication. For example, we had a really good conversation here on what authentication technically means, and I think that would be a major step that we could work on a document on what authentication is and what it should require, and also look at authorization as we come from the necessity, proportionality, and legitimacy, and see how technically the submission form can have these properties to make sure that the request is legitimate and proportional.

Another thing that we could work with SSAC on is to look at your advice and see what sort of human rights impact it could have. It can have good positive human rights impact, or it could have maybe some you need to also consider some kind of mitigation mechanism, but we can do that. We can work together on a piece of advice that you're working on, and also some of the stuff that you have been doing recently on the ISP blocking and overblocking that could lead to censorship. These are the things that we really care about, so we can work on that together as well for us to bring the human rights perspective.

RAM MOHAN

Thank you so much. This has been a very useful session. One thing I'm thinking of is just as a way to learn this and kind of try it out, Rafik and Farzaneh, maybe we take an advisory that the SSAC has put out, and we use that as a case study to say, if you were to apply a human rights framework to it, what would we think we should add or change to it? That might give a worked example of learning by doing, which might then help for future work. I would say, intercessionally, we should sit down and identify maybe one document that might be suitable for this, and then do an experiment on it.

FARZANEH BADIEI

That's great. If we can have a conversation about authentication, continue doing that. That would be a good thing.

RAM MOHAN

Sure thing. Thank you. Let's go to the very last piece of our agenda, which is simply something that I wanted to share with you. The SSAC is doing some work with the ISPCP on a training series. We're doing that inside of the community. This gives you a sense of what we have been doing and what we are continuing to do. These are topics where the ISPCP sets the stage. They bring the audience, they do the coordination, they do all of that part of the work. What the SSAC is doing is bringing our expertise, our advice, the people who actually know about these topics. They're coming into those webinars or conversations in person.

Here, Tara, for example, is going to be doing work on privacy versus security. We're doing that as a collaborative effort for the entire community. Something to think about because you have things that are of interest. We've been talking about how we can do things together. A model that works well for us is to leverage the work that we've already done and the expertise that we bring and to take it into your communities and to inform or amplify as necessary. No action here, but information for you now so that we can think about what we do next. Rafik.

RAFIK DAMAK

Okay, thanks. If I stand correctly here, we can have some idea that we can ask the SSAC to present to our group or larger or wider

community. I think we can do that and we can come up with some list. Yeah, looking forward to that.

RAM MOHAN: Great. That brings us to the end of at least our agenda. Anything more for you to add, Rafik?

RAFIK DAMAK: Yeah, thanks, Ram. I hope that was a useful session. I know that maybe there are some disagreements in some area and agreement in others, but that's the main point of having this interaction to share and to listen and to work on that so we can update in our position and to share later on what we think. It's more about cooperation and cooperation moving forward.

RAM MOHAN: Great. Thank you very, very much. That wraps this session up. Thanks.

ANDREA GLANDON: Thank you. You can stop the recording.

[END OF TRANSCRIPTION]