ICANN84 | AGM – GNSO: NCSG Discussion on DNS Blocking and Human Rights
Saturday, October 25, 2025 – 9:00 to 10:00 IST

ANDREA GLANDON

Hello and welcome to the NCSG Discussion on DNS Blocking and Human Rights. Please note that this session is being recorded and is governed by the ICANN Community Participant Code of Conduct, ICANN Expected Standards of Behavior, and the ICANN Community Anti-Harassment Policy. 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 otherwise as directed. When speaking, please state your name for the record and speak clearly at a moderate pace. And I will now hand the floor over to NCSG Chair Rafik Damak. You may begin.

RAFIK DAMAK

Okay, thanks, Andrea, and thanks everyone who made it today in one of the first sessions of this ICANN84 in the Dublin meeting. Today, just to give a quick introduction, we'll try to discuss about DNS blocking in the context of ICANN. And kind of maybe to give more context is the idea originated from when we saw the report that was made by the SSAC and that was shared prior to the ICANN

meeting in Prague. And here we thought that can be a good opportunity to discuss about DNS blocking and to try to bring kind of to share about cases and examples.

So for that purpose, we'll try to go or to follow this agenda. First, to get more technical overview and we count here on our colleagues from the SSAC to give more explanation about the techniques that they are using for DNS blocking. And then we move to share all the real-world examples and some case studies just to make it clear what is happening exactly in the different part of the world. And at the end, we'll have that facilitated panel discussion. So that will be an opportunity for Q&A, for comments and so on.

So, this is how we will do for today. And just to share about this session that it's organized by NCSG in cooperation with the CADE project. And for that, I would like to ask Stephanie to share a few words about or to introduce the CADE project.

STEPHANIE BORG PSAILA Thank you, Rafik. It's a pleasure to be at this ICANN meeting. So, the CADE project, the Civil Society Alliances for Digital Empowerment, it's a multi-year project co-funded by the European Union. We're a group of nine partners from around the world. And we are working together to improve the engagement of civil society actors, especially from the global south, to participate in digital policy processes, including ICANN. And in fact, we are currently supporting INSM network from Iraq and some from Palestine to

engage in this AGM. And you will hear from them later in the session.

So, our goals are very clear. We don't want to repeat what has maybe not worked in the past. We want to improve and build on the success stories of other projects. So, we took a very close look at what has worked. We're building on that. And in these four years of the project, we are hoping to see much more engagement from CSOs from the global south.

So, this is what you will hear today from our colleagues is a prime example of the engagement that the project has made possible. So, I'll stop there and give it back to Rafik. Thank you.

RAFIK DAMAK Thanks, Stephanie. And with that, I will pass here to Michaela to do the moderation and to go through the rest of the agenda. Please, Michaela.

MICHAELA SHAPIRO Thank you, Rafik. Thank you, Stephanie, for being here and for your introduction to the project. Thank you all for turning out on a Saturday morning. It's really appreciated. Feel free to move up to the front if you're feeling comfortable and excited about the topic. Otherwise, no problem. I just wanted to encourage all of you as well as we go through these presentations today to hold on to any questions or any nagging thoughts you might have that you'd want to bring up later.

We'll have a portion where we'd love some audience Q&A. So, just file that away. Do with it what you will. But we are incredibly lucky to have a number of speakers with us today, starting off very strong with the SSAC, represented by Ram here to my left, who will be giving us a little teach-in that we're really excited about to kind of set the scene and give us the technical background for this discussion.

Then we'll move into these real-world case studies of incidents of censorship that has taken place at the level of the DNS, where we'll have Farzaneh, the brilliant Digital Medusa NCSG rep today. She'll give us a presentation here live. Then we'll move online to Jalal. And then we'll move to Hamzoz, who is also, we're very grateful, is here today. His first ICANN, so we're very excited. Please give him a warm welcome if you see him around this week. I will give a short presentation about some of our work at Article 19. We'll have a very brief, kind of facilitated panel discussion, moderated by myself. And then we'll go into audience Q&A. So, as I said, please keep some questions in mind. We're really excited for it. So, with that, I'll turn it to Ram. Thank you.

RAM MOHAN Thank you so much. Good morning. I'm Ram Mohan. I'm the chair of the ICANN Security and Stability Advisory Committee, SSAC. And if you could please go to my slides. So, I'm here to provide the technical underpinnings of this topic and what we're talking about, especially what the SSAC means when it says DNS blocking. So, in

my brief presentation, I plan to cover really four areas. The next slide.

What is DNS blocking? Why did the SSAC visit the topic and issue SAC127? What are the unintended consequences of blocking? And our recommendations. On the next slide, let's understand how the basic process of DNS resolution actually works. So, for all of us who are here, we understand that when you type something into a browser, it just resolves. But there's multiple steps along the way and multiple parties along the way.

The places where we tend to look at on the next slide is where DNS blocking often occurs. On this slide, you will see, the next slide, please, you will see that one of the most common places, I'll just keep speaking to it. One of the most common places for DNS blocking to be implemented is at the recursive resolver. That's typically in the cloud, and that's one of the most common places for the blocking to happen.

But it also happens, on the next slide, you will see that it also happens in what we call on the wire. This is the network paths that link your home or enterprise to the cloud, to the DNS resolver, or from the DNS resolver to the actual authoritative DNS server. So, what does that actually do?

On the next slide, there are multiple things that could happen. A DNS blocking system could deny that this address that you're looking for actually exists. It could say, I don't see a listing for ICANN.Org, it just is not there. Or, on the next slide, it could say it is

at a different place. ICANN.Org is at a different IP address altogether. So, that looks like it's not blocking, but it could give you a fake address or a redirected address. And it could be a warning page, but it could be something else also. And on the next slide, it could also give you no answer at all. You could just encounter blank space, right? The connection just hangs, and you don't know what's actually happening.

So, on the next slide, you'll see, why is it used? It's really, there are three primary reasons that the SSAC believes it's used. For security, for content control, or for legal and political reasons. And in some cases, it is all of the above. Some cases, it is some of these three reasons, right? So, next slide. So, when we produce SAC127, and even here in this conversation here, we're not taking, you know, any position on whether DNS blocking is legal, not legal, you know, is it moral, immoral? That's not the focus of the SSAC. Our focus is really on what it is and what it could do. So, next slide.

The SSAC has studied this topic for a while. We published a report, SAC050, many years ago, and then SAC056. And in those reports, we established some core principles of blocking, right? The first principle is, do no harm. It should not negatively affect users and networks, outside of the blocker's administrative controls. So, try to keep the scope of the blocking as limited as possible. The second thing that we also notice, blocking is often ineffective. And finally, blocking can cause unintended consequences.

Next slide, please. So, what has, from the time we published SAC050, SAC056, to the time we published SAC127, what's happened? What's become mainstream? What's become mainstream is that circumvention is now, in many places, is the norm. And DNS traffic itself is becoming invisible.

So, the ability to look at what is happening at the DNS is much more difficult for network operators. At the same time, government rules and government roles have become far more complex, right? So, these are what is state-of-the-art right now. We have some findings to share. First, it's a blunt instrument. DNS blocking does not remove or alter the underlying content. And so, the next slide, what you see is that content remains available. And if you're a determined user, there is a way to reach that content.

On the next slide, DNS blocking is often also ineffective. Circumvention methods are much more mainstream and far more accessible than when we wrote SAC050 and SAC056 in 2011. There are alternative DNS resolvers. There are virtual private networks, VPNs. And so, there are multiple ways now to overcome pervasive DNS blocking.

Next slide. This is kind of ironic. We believe that DNS blocking can actually weaken security. What happens here is users start to ignore, they start to normalize browser security warnings. We are teaching users with DNS blocking to ignore these warnings and to get past what are intended to actually protect users, right? And it also reduces network visibility, right?

So, it's much harder to detect computers that have been infected with malware or to be able to fight large-scale cybercrime. So, with all of these findings and observations, what has the SSAC actually said? We say in SAC127, on the next slide, we say three fundamental things. First, if you're a regulator, if you're somebody who intends to implement DNS blocking, please understand what that technology actually means, what it does, right? And you have to see whether that method, DNS blocking, will it actually fulfil its objectives.

The second thing is minimize collateral damage, right? This is a callback to what we said as an original principle in 2011, which is to keep the scope of your blocking as controlled as possible, right? So, that's the second thing, minimize collateral damage. And the third thing that we recommend is to be transparent about it.

Okay, you have to block. We understand that there are multiple reasons for it, but it's actually not just polite, but it's actually important to say you're blocking. And there are some new technology pieces that allow network operators and other users to say that the traffic is being blocked for a specific reason, right? So, that's what we're saying. And that really is the end of the teach-in.

The final slide that I have gives you a QR code. It's a real QR code. It's not an attempt to phish you. And it'll actually take you to that SAC127 slide, to the SAC127 report that you can download. Back to you, Michaela.

MICHAELA SHAPIRO Thank you so much, Ram. And just to reiterate again, if you had any kind of follow-up thoughts or questions for Ram and on his presentation, feel free to hold onto them for later in the session. So, thank you so much, Ram. I'll turn it to Farzaneh now.

FARZANEH BADIEI Hello, everybody. I'm Farzaneh Badiei and I'm a member of the Non-Commercial Stakeholder Group. I'm also on the GNSO Council. And I run Digital Medusa, which wants to keep people online, safe, and their human rights intact. So, I did some studies on DNS resolvers and blocking and how that can affect people's access to online services. And generally, the effect on internet freedom. That's my LinkedIn QR code. And the other one is the report.

Next slide. Next slide. Yeah. Sorry for these naked slides. I wasn't in the picture mood. So, the findings of the Digital Medusa report is that DNS resolver level blocking is growing, often without transparency or due process. If public resolvers become more concentrated, and by concentrated, we mean that there will be like just only few actors that provide DNS resolvers. It raises risks of coercion, policy capture, and fragmentation. Blocking at the resolver or naming layer can unintentionally restrict access to legitimate contents or services.

We keep using this term collateral damage. And I think that we should change that term. We actually have innocent users that cannot have access to online services. And their freedom of speech sometimes is hampered. So, it's more than collateral damage. It's people that get oppressed.

There is a clear need to keep DNS governance technical interoperable, and open to preserve internet freedom. And this work was done in the data analysis was in collaboration with .ie. They are, I don't think they're here. I think they're in bed. But I just wanted to thank them. Next slide. And this is the QR code for the report. Yeah, so when do DNS, so DNS resolvers actually can empower freedom.

In countries where ISPs block websites at the DNS level, users often switch to public resolvers such as Quad9, CloudFlare, Google DNS. These resolvers typically do not implement, well, some of them do not implement local blocking lists, allowing users to reach sites otherwise filtered domestically. And the resolver report shows a strong link between public resolver use and internet freedom score.

Countries with lower internet freedom disproportionately have high use of public resolvers. And this is not, I'm not claiming a causation or even a strong correlation. We are still looking, but we are trying to see if during, for example, political uprising, the use of these public resolvers will be increasing as well or not. Next slide.

So, some of the problems with the DNS blocking is that intellectual property lobbyists, they lobby the lawmakers. And there are many terrible laws that have come into effect. Italy's piracy shield is one of them. And the initial blocking that happened in, so they actually allow blocking at the DNS resolver layer.

So in October 2024, Italy's piracy shield law caused a temporary block of Google Drive, which affected thousands of people access to their Google Docs and Google Drive. These were not like malware or phishing domains. They were shared research or workspace blocked by automated system and on transparent block lists. That's another problem that we have. We never know how these block lists are curated and how they are actually implemented, how they are reviewed, and how the ISP or the public resolver uses them. And so next slide.

So what does that have to do with ICANN? So, ICANN's mission is to coordinate the policies for allocation of domain names, not to regulate content. It's in the ICANN bylaws and we will keep it like that and over our dead bodies if we want to regulate content as ICANN. So, DNS Abuse policies or any other policy should stay narrowly focused on security and stability. Should not be repurposed for content moderation. So, the DNS Abuse definition should be technical and limited.

When ICANN's contract with registry and registrars or its compliance mechanism starts incorporating measures that lead to content related mission creep occurs and turning a technical

governance into content control. And we see what happens when we try to control content at the DNS level, which can be very disproportionate and affect people. So, the next slide.

So, the key risk is the mission expansion. And also, we had a session a few years ago, we had a few sessions about these voluntary Public Interest Commitments, especially for New gTLDs. It can become a de facto regulatory tool if not clearly limited or if voluntary commitments become expected norms.

At NCSG we were quite vocal about these voluntary Public Interest Commitments not to make ICANN a content regulator. And our recommendations, which is on the next slide, keep ICANN's role strictly technical and rooted in DNS security and stability, separate technical abuse from content regulation, content abuse, promote transparency and due process in any blocking or sub suspension decision, encourage diversity, decentralization of these resolvers to reduce the risk of single point of control, maintain clear limits on picks, and New gTLD obligations to prevent content-based enforcement through contracts. And that's it. There's a last slide, and I have a beautiful picture for you there.

MICHAELA SHAPIRO Thank you. Perhaps while we wait… ah, beautiful slide, you were correct. Thank you so much for that. So, for now, just for the sake of time, I would love to turn to our fellow Jalal, who will be coming in online. Can I just check, Jalal, that you're able to come in?

JALAL ABUKHATER I'm on. Can you hear me? Can you see me?

MICHAELA SHAPIRO Yes, thank you so much. Please go ahead.

JALAL ABUKHATER Okay, fantastic. Happy to be speaking to you all. Thanks for the invite. Honestly, to be more familiar with ICANN, it was a new task for me. My name is Jalal Abukhater. Currently, I am the policy manager at Amleh. Amleh is a digital rights organization based in Haifa, focused on digital rights of Palestinians. What started off as an organization that looks specifically on online platforms, content moderation, how companies are failing in respect of obligations for human rights, etcetera.

With time, our focus shifted a lot towards other aspects of digital rights violations, whether it's infrastructure level violations or surveillance and data collection, that is all of those human rights abuses. For the purpose of talking about censorship risks, I'd like to talk about the context. It could be something helpful for others to understand the context.

In the digital space, access is deeply entangled with systems of occupation and control. There is no sovereignty that we can talk about at this level. Censorship extends beyond social media platforms and is, of course, structured level on a major level.

Regarding DNS blocking and infrastructure control in our context, we have to state the facts first. Israel retains full control over the ICT infrastructure that is a response to the global internet, including international gateways, spectrum and physical routing. There is no sovereignty for Palestinians in this regard.

Palestinians do not have sovereignty over the DNS or telecommunications service providers rely fully on Israeli controlled backbones. This allows technical blocking at the infrastructure level, such as throttling, DNS blocking, and total service disruptions, as we have seen repeatedly during the genocidal war in Gaza in the recent two years. The blackouts occurring in Gaza were not just caused by deliberate actions and destruction of fiber routes. It is also a sign of how Palestinians are structurally excluded from managing their own internet in general.

Regarding censorship of civil society, Palestinian human rights organizations have their domains of hosting restricted, especially in the recent months due not only to Israeli actions but also to these actions by the Trump administration in the recent period, particularly against human rights organizations who've been working with the International Criminal Court.

So the sanctions have been levied over multiple very prominent human rights organizations such as Al-Haq, Al-Mizan, the Palestine Center for Human Rights, because of their work with the ICC, reporting war crimes and other violations to an international legal body. They risk being de-platformed by US-based providers,

whether it's GoDaddy or others, because of this sanction's regime, which demonstrates a new level of DNS control that's perhaps something not familiar to many in different contexts. But in our context, it's something that puts more pressure on those organizations.

And the sanctions regime can silence this critical and vital documentation of human rights violations. But I have to mention that there is also a problem of domestic censorship that does exist very heavily. The Palestinian Authority, as the authority with the formal level of authority in the occupied territories, especially in the occupied West Bank, there is a cyber crime law which has been used, exploited in a negative way, in a malicious way, to block news sites and activist pages via ISP blockings, often implemented through DNS filtering.

I'm talking about even Al-Jazeera.net, for example, a news website that was blocked. The Arabic version was blocked recently using the cyber crime law. This is a reality that is perhaps common in many Arab countries. In Jordan and Egypt. But we're also witnessing it in PA-controlled, by PA-controlled ISPs, Internal Service Providers.

In regards to broader implications, DNS blocking and domain takedowns can become tools of political repression, as we see in Palestine, especially where there is no transparency or appeal mechanism. In contexts like Palestine, where connectivity and expression are already constrained by the military occupation,

even small interventions at the DNS level can have major consequences, including erasing documentation, cutting communication, isolating entire populations digitally.

For the space of ICANN, what we hope to encourage is to acknowledge the geopolitical risks of DNS-based content controls. We encourage the support of human rights due diligence by registrars and registries, especially regarding state or sanctions-driven takedown requests. And of course, to uphold the principle that technical infrastructure should remain neutral and accessible, even in a conflict setting.

So, I believe ICANN does have a role in ensuring stability and neutrality of the DNS. And this carries immense human rights implications as well. For Palestinians, digital access has become a matter of survival and visibility. And that's why I'm hoping that by presenting this case study, this understanding can be helpful for us to recognize the issue and to work towards finding solutions. I appreciate the time. Thank you so much. And I'll pass it back to the chair, please.

MICHAELA SHAPIRO Thank you so much, Jalal, for the really useful examples that you just shared. And thank you so much for joining us. We're excited to have you at ICANN. So, now I'll turn it to Hamzoz, who's in the room with us.

HAYDER HAMZOZ

Hello, everyone. Thank you so much for including our voice, the civil society here in this session. I'm glad that we are part of this amazing Project K to include our voices here. Thank you so much. This is my first participation in ICANN and first session, so I'm a little bit nervous, so I apologize for that. And let me explain more about our role.

We are Digital Rights Defenders, a network that was established back in 2011 in Iraq, where difficult to explain to the people what is the digital rights, that they have the rights to express about themselves online, you know, because they access to the social media just to, you know, entertainment. But we have a role here to explain and increase the awareness of the people. So, that's why we established this network, NSYM, to raise the awareness and also protect the people rights and the internet users' rights on the internet.

Let me give you more about some history about governmental actions, let's say, against the free digital space we have in Iraq. In August 2023, the Iraqi government proposed a cybercrime law, which sparked a lot of discussion among members of the parliament due to severe violation on human rights. Example, the law included a life imprisonment for anyone who deliberately uses computers or information networks to undermine the country's independence, unity, security, or interest. They just leave it like this.

It's also imposed disproportionate fines and punishments used vague terms and lacked clear legal definition. And the fines, it could be up to like $10,000 for each article. And on the other hand, also Iraqi authorities continue to crack down on online content through the platform Ballagh, and Ballagh in Arabic means report platform, that launched in January 2023.

We're encouraging Iraqi audience to report any content they don't like, a content creator on any platform to report there. And between February and August 2024, around 152,000 reports, complaints were filed through this platform, which allow, as I mentioned, individual to report content on social media. And based on that, they will try to issue an arrest order to arrest these content creators. And multiple people have been arrested for just criticizing the government or also just expressing about themselves because they are just dancing or, these kinds of contents.

Also, as you know, Iraqi governments regularly shut down the internet during exam periods to, I'm sometimes embarrassed to mention that, just because to prevent the students from cheating in an exam. So, it's an entire shutdown in the whole country. That behavior is also practiced in Kurdistan region, which is they have different system, different policies, but same actions.

So, they've blocked the internet and they shut down entirely, even on the banking system, government agencies, everywhere, for two hours. And this is, you know, beside the harm to the human rights, it's also an economic harm, which has cost around $209 million and

lost in the current for each shutdown, which is usually last for two weeks. Imagine we have three rounds of exams each year, round one, round two, and round three for the students to pass the exams.

Each round, they do that kind of exams and each also level. So, we are in the top level of internet shutdowns in the whole world, comparing to the number of shutdowns happening. Also, recently, that's happened just two days ago. I just came from Baghdad, where is GBS jamming also happening in Iraq to protect the upcoming election on November 11th, where all people now lost.

We have today a session in Baghdad, people, the participants, they couldn't use Uber or these similar apps to get online taxi to come to their training center. And the delivery people, they cannot deliver items. So, it's really a mess and people, they don't know what's going on here. They thought this is like some action from outside actors and without any explanation what's going on. And it's still ongoing.

And this is a new practice happened, to be honest, in Iraq, which is the GBS jamming. I will jump to also the Iraqi government action and the plans to block the Google domain name system, DNS server in the country. And blocking access to Google DNS creates a ground of cyber attack and hijacking attempts, but especially if it's a weak security measurement are implemented, which is that's what's happening in the case of Iraq.

And this unencrypted setup would prevent query data, as you know, from being securely encrypted and allow for tracking of individual and their data, unlike Google DNS, which does not store U.S. user data when used. The local system could expose users to privacy risks.

DNS Abuse has been used to block some news websites like Ultra Iraq in November 2023. And this has been reported in our report we usually do annually with the Freedom House. You can refer there to get more details on Freedom on the Net report with the Freedom House.

Also, that DNS blocking from legal standpoints, a decision to block it conflicts with the Iraqi constitution, Article 40 and 46, which is guaranteed the protection of communication freedom and including electronic correspondence. The DNS blocking decision contracted this article for two reasons. First, it's not established by a law. And second, it's infringed on the fundamental rights of the internet users, including freedom of expression and privacy on communication data.

Finally, these actions that happened by the Minister of Communication recently also to threaten to ban TikTok and other social media platforms if they do not collaborate. And also, they just blocked last week Roblox, the online game. And all this, you know, because, again, people, they don't know what's going on. So, they said, we are blocking that to protect the Iraqi families and values. And people, they will say, oh, yeah, because we still, you

know, in a mindset where government should be responsible on people's life, people's protection and ethics. And this is our parents, the government, and they should protect us.

Finally, I close mark that all these violation decisions, it's in a breach. As you know, in Article 19 of the Universal Declaration of Human Rights, and the ICCPR, both guarantee the right of the freedom of expression and the right to seek, receive, and impart information through any medium of people's choice. Thank you so much.

MICHAELA SHAPIRO

Thank you so much, Hamzoz. Very hard acts to follow. So, thank you all for sharing these examples. So, I'm going to try my best to kind of just find an overview to kind of talk about a little bit about what we to kind of summarize a little bit of what we've discussed today. So, I would love to go to the next slide, if possible. And just to quickly summarize so far, right, we've had a presentation from SSAC, who's discussed and helped us distinguish between the kind of technical elements of blocking versus, for example, domain suspensions or deletions, and the different actors involved in that space.

We've had from Farzana, an overview of her research and on DNS resolvers and their role in potentially facilitating censorship in certain cases when it's wielded as such. And we've had real world examples presented by speakers from Iraq and from Palestine who have given us that sense of what is happening on the ground when

we talk about the risks of intervening at the level of the DNS. And a lot of this is probably not new to those of us in the room.

So, I'm not going to try to oversimplify the discussion. But just to say, you know, one of the reasons why I really wanted to organize this session, I was so grateful that the NCSG was interested in supporting that idea, was we kind of when we think about content moderation, we often think about the level of social media. And we think about what the decisions that are being made by either government, social media or other regulatory actors, having an impact on the availability of content. But we often don't think about the role that infrastructure providers can play in either facilitating or potentially to the detriment of the availability of content.

And as SSAC in the report really helpfully laid out is the kind of the actions that you can take at the DNS can either be used as tools, they are just simply tools, I should say. They're the way that they are wielded will then decide what happens from there and the implications going forward. So, we at Article 19, who I'm representing today as part of, we are members of the non-commercial stakeholder group, we've been involved at ICANN for a while now.

And we noticed that there was a gap in the literature when it comes to understanding the role that different infrastructure providers play, but specifically the roles that registries and registrars play. And in trying to grapple with DNS Abuse mitigation and finding that

beautiful balance between addressing the very real harms of DNS Abuse, which we have already very helpfully outlined in ICANN's definition of DNS Abuse, and then finding that balance with upholding safeguards online, including the freedom of expression online.

And we wanted to be able to speak with a number of actors, including civil society actors, like the ones who are here today, as well as the registries and registrars who keep our DNS running. So, a lot of you in this room, I've already even spoken about some of your policies and how you're thinking through what to do when it comes to either requests for domain suspensions or takedowns, or how you're handling DNS Abuse in your area.

So, if we could perhaps go into the next slide. What I've tried to do is kind of just outline a few of the different examples that we've been looking at that were flagged to us about when it comes to DNS domain suspension requests and the implications that that has on the media and the availability of news and journalism online. So, this was an example in India, we became aware of three different environmental groups who were targeted and their domains were suspended without any notification. And this came ahead of a consultation organized by the government on environmental justice bill.

And they took a while for them to figure out what was happening. As those of us in the room might know, when it comes to a website isn't loading, there's a number of different ways in which that could

have happened. But through some of their own kind of technical magic, they were able to figure out that this was in fact a domain suspension.

And I wanted to flag this example because I thought it was both I was able to speak with some of the activists involved in this and the ramifications for their ability to organize and to be able to respond in a timely manner to this consultation by the government was severely impacted through the inability to have their website be made available.

So, the next slide, I'm not even going to attempt to try to read this because it is in Belarusian. So, once it gets there. So, this is from an article that discussed the Belarusian Association of Journalists, who similarly their domain was also the delegation of their domain was also suspended without notification, without justification, or at least the justification was that they detected some kind of violations of the cyber laws in Belarus.

And the idea being that they, the organization of journalists were reporting on things that perhaps the president of Belarus was not so thrilled about. And I highlight this example to showcase that these ramifications are not only just about getting news and spreading information out there, but it also has democratic implications and implications for upholding democracy.

And the last example I'll get to going to the next slide, please, is about Catalonia. And this was a raid on the registry that controls .cat, the Spanish government, the police raided their offices. So,

we're seeing a real world kind of impact of very literal seizure of the domain in some ways to try to stop the resolution of the .cat top level domain, so that they were not able to share information ahead of a referendum, on the their independence referendum. And this was in 2017. And this was published by EFF, the Electronic Frontier Foundation. So, all these examples, oh, and I realized I actually have one more.

So, one more slide. This is about Nicaragua, and very similar to the ones I've already highlighted. But this was also an example of trying to prevent the resolution of websites being made available through the .ni domain. And this affected three different, or sorry, four different news organizations based in Nicaragua. And yes, as Farzaneh mentioned, Michele has also mentioned a lot about this as well, and would be very happy to have him come in perhaps in the Q&A if he's so inclined.

For the sake of time, I don't want to take up too much more. But going to my last slide, I very shamelessly stole this from Norad, who I thought just very helpfully in a very pretty graphic laid out, who are the different actors involved when it comes to thinking about content being made available online? And just to say, you know, why are we discussing this today? And why are we discussing this at ICANN? Because some of this obviously goes beyond ICANN's bylaws and the purview of some of these organizations that we're discussing today.

The reason is because we are now in the process, as this will not be news to anyone in this room, but we are discussing DNS Abuse yet again. And we will be discussing a potential policy development process on DNS Abuse, hence why we wanted to have this discussion, because we thought it's important to recognize that what we discussed today has implications beyond just the rooms in which we are in at the moment.

And so, I wanted to end with just a few kind of concluding thoughts that when speaking with a couple of registries about this topic, one of the really great metaphors that was used was when you think about using the DNS for the purposes of content moderation, it's like taking a sledgehammer when what you really need is a screwdriver. And I thought that really nailed, you know, why this is using the DNS for content moderation can be so problematic. And SSAC laid that out much more eloquently in Ram in his presentation about the risks of the kind of over blocking and the ramifications that could come from using the DNS for content moderation.

And a couple of thoughts that I wanted to end on is that, we really, from speaking as well with others in this space, is realistically registrars and registries in this room, and they can speak for themselves, but the sense I've gotten is that they don't really want to be doing this. They don't want to be content moderators. That's not the role that they want to play. And for a lot of the governments, a lot of the CCs involved, that's actually enshrined whether in their bylaws or their terms of service, I should say, or

even within court cases, depending on the country we're discussing.

So, that's not a role that they should be playing. And we don't want to put them in that role. Similarly, when it comes to, it's not even necessarily efficient, as also Ram pointed out in his presentation. And just one recommendation that I'd want to put forward is, we've been thinking within Article 19, a lot about the role of transparency and transparency reports. And this is also something that came up in SSAC's report, that doing kind of due to the invisible nature of infrastructure providers, there are different mechanisms that we could use to try to make this more transparent when you are trying to address content and the last recourse is and should be taking action at the DNS, whether it's a domain suspension, deletion, or a block.

And the idea being that we can also find ways, there is some work going on, for example, at the Internet Engineering Task Force, to try to develop error codes to be able to provide some transparency as to why a domain is no longer available. So, we've talked a lot. And so now I had envisioned originally a panel discussion, but I wonder, for the sake of time and seeing the chat, there seems to be a lot of interest coming from the audience.

Perhaps if the panellists are okay, I could open the floor to some questions from the audience. Fantastic. So, people, please feel free. I don't know if there's hands online. I think I see one already from Sourena. So, please feel free to come in and turn on your mic.

SOURENA MAROOFI Hi, my name is Sourena. Can you hear me?

MICHAELA SHAPIRO Yes, we can hear you.

SOURENA MAROOFI Okay. Thank you very much for the presentation. I have a question for Ram. So, in the presentation and also in the SAC127 documentation, I saw that one of the ways is to change the IP address for DNS blocking and redirecting the user to another page showing that this page is blocked or showing the appropriate message. So, isn't it against the HSTS and TLS encrypted domain names, which actually work since 2006, 2007? So, it should be impossible with HSTS and TLS encrypted enabled domain names to redirect the IP address and show a web page because the browser doesn't let you do that. So, how come this is one of the approaches that DNS blocking servers can use? Thank you very much.

RAM MOHAN Thank you. Yeah, I think it's difficult, but it's not impossible. And in fact, what you'll find is that browsers will throw up a warning saying, are you sure you want to go there? And users end up clicking through and actually getting there, right? So, they don't actually stop you, but they give you severe warnings. And this is one of the things that we talked about, right? By blocking, we're

now training users to ignore real issues. And they get used to this. And then when there is a real problem, they click through and then they get phished, they get malware, they get other problems that come through straight to them.

SOURENA MAROOFI In fact, I think that in the case of wrong TLS encrypted, the browser will show you a warning which can be bypassed. But in the case of HSTS enabled domain names, there is no way to redirect. So, there is no warning from the browser.

MICHAELA SHAPIRO Thank you so much, Sourena. Perhaps we could take that part of the discussion offline just to give some space to others. So, I see Bruna has her hand up. Please go ahead.

BRUNA SANTOS Thanks, Michaela. Just very briefly, I just want to take the time to thank you guys for organizing this. Over the past years, we have been listening that, you know, a lot of the discussions around Palestine, DNS blocking, the Middle Eastern region, and so on, were way too political to be at ICANN.

So, I just really wanted to take the time to thank both Hamzoz and Jalal for being in this session, because I don't think both your perspectives is highlighted enough in this space. So, really, really thanks for that. And the second point I will just post it on the chat,

but this session was incredibly connected to the work we have been doing at the Policy Network on internet fragmentation.

And currently, we have some recommendations for review, just in terms of like how stakeholders should be collaborating, what's expected from the different parts involved in the both the infrastructure stack, but also the content stack. And it would be lovely to hear feedback from all of the speakers, including you and Farzaneh on that. So, thanks a lot.

MICHAELA SHAPIRO Thank you. Go ahead, Farzaneh.

FARZANEH BADIEI I had a question from registries and registrars. Do you want to give us examples of blocking orders or takedowns that you received? No? Oh, yeah, Michele, go ahead.

MICHELE NEYLON Thanks, Farzaneh. It's Michele for the record. I mean, sure, like under the current sanctions regime from the EU, there is a list of domain names associated with Russian state media, that all ISPs across the European Union are meant to block at the resolver level. When that was initially pushed out, I think it took some other ISPs a little bit of time to implement it.

And I'm not even sure how that was communicated. We found out through ICO. If we hadn't got a notification from ICO, I don't

actually know how long it would have taken the Irish government to actually bother to tell me. Because the commission would probably have been the regulator for that. But right now, it's a bit of a hot mess in terms of who our regulator is for what.

You mentioned the Catalan thing previously. So, that was that was a bit of an interesting one, because a lot of the .cat domain names that were being used by those involved in that were registered through us. So after things settled down, it went to the Spanish Supreme Court. I think the judge spent about half an hour arguing with various people because they couldn't wrap their brains around the idea that the Internet is global and that a person living in Barcelona could register a .cat domain name with a registrar in Ireland. And who the hell was Black Knight? And what the hell were they doing? It's quite funny.

So, if you want to be mentioned in the Supreme Court in Madrid, check that one off your list. But I mean, generally speaking, I think in Europe, we don't see as many blocking orders as you do in certain other jurisdictions. But as I think as others have said, I mean, we don't want to be content moderators. That's not our role. But I think one of the first takedowns that we received as when I started out 20 plus years ago, was from somebody saying that there was a website we were hosting that offended somebody in Chile. And I was like, well, I'm not in Chile. So, you know, they send me something from a court, maybe over here, I might actually care. But until then, no.

MICHAELA SHAPIRO Thank you, Michele. And I know there are a couple more questions. So, I encourage you both to send those separately after, because I'd like to take the moderator's privilege of asking one question to our panellists before we close off. And I'm going to keep it short and simple. With the remaining five minutes in one sentence, what is one thing that participants you'd like for them to take away from today's session? And if it's all right, maybe I'll call on Ram first, if you're comfortable.

RAM MOHAN Thank you. Exercise care. This is a blunt instrument. It can cause lots of unintended consequences.

MICHAELA SHAPIRO Thank you.

FARZANEH BADIEI Farzi, would you like to go next? Ram just said what he wanted to say. Come on. So, we don't want control, especially at infrastructure level, and we do not want the excuse of, yes, we are fighting with some malware or botnet and stuff like that. There has to be transparency, there has to be accountability from the government, as well as the other actors.

MICHAELA SHAPIRO Thank you. Perhaps I could turn to Hamzoz.

HAYDER HAMZOZ Yeah, I think two things are important. I echo the transparency issue. I think it's very important. This is part of the education purposes for the participants. And also, I think digital literacy, it's an important thing, because this will bring more voices, local voices, into our movements.

MICHAELA SHAPIRO Thank you. And if we have Jalal still online, would you like to come in? If not, I'll come in to say, and also similarly, I think Ram and Farzaneh still what I was going to say, but just to say that I hope that we can use this as a jumping off point for the discussions to come the rest of this week.

Our intention with this session was just to shed light on some of the kind of potential consequences of this. But we also want to make it very clear that this is not to blacklist anyone. This is not to point fingers at anyone. This is very much an exercise in trying to understand what are the consequences when this tool is wielded for potentially dangerous consequences. But at the same time, we are well aware that the vast majority of those of us who are in this space are not wanting to act this way.

So, really appreciate coming in with an open mind. Thank you for this time. And unless there's anything that the chair from the NCSG wants to come in to say before we close off. Oh, this is just an hour

session. Oh, sure. Yeah, I can take a question. Sure. I see a hand up in the chat. Please go ahead. So, this is for, I believe it's for Cliff who has their hand up. Oh, sorry. Then go ahead, Jeff.

JEFF BEDSER Actually, I put my hand up for LJ because she didn't have her computer. So, go ahead, LJ.

LAYAL JEBRAN So, Layal Jebran from SSAC. I'm going to remove my technical hand.

MUTEGEKI CLIFF Hello.

MICHAELA SHAPIRO Oh, please go ahead.

MUTEGEKI CLIFF Hello. Can you hear me?

FARZANEH BADIEI Yes.

MUTEGEKI CLIFF Yes. Hello.

MICHAELA SHAPIRO Yes, we can hear you. Go ahead.

MUTEGEKI CLIFF All right. I just had one question and I'd put it in the chat, but let me just get out here. And the question is considering that domain registrars and registries operate globally. How can we avoid conflicts between national content restriction orders and ICANN commitment to a global interoperable internet?

MICHAELA SHAPIRO I don't know if there's someone on the panel who would like to take that question. Go ahead, Ram.

RAM MOHAN Thanks. I think it's a good question, but it's kind of a fundamental issue, right? Governments and jurisdictions exercise their rights within their jurisdictions. But the thing that sometimes is missed is that effect that in the real world, in the non-internet world is often restricted to jurisdictions. When you apply it to the internet world, it crosses over and it spreads globally. So, that's a fundamental issue. And I think one of the important things is for regulators to understand that the impact of their decisions locally could actually and often are global.

MICHAELA SHAPIRO Thank you. And then did you want to come in?

LAYAL JEBRAN Still have time? Amazing. So, I was mentioning I'm going to remove my SSAC cap and go more on the humane side. So, I really appreciate what Jalal and Hamzoz mentioned. I interact with them in different spaces and they're great people and they do great things. One thing I wanted to mention is that maybe, so I'm from Lebanon, so this is close to home. Maybe people in Europe and the USA do not get across this a lot and it doesn't affect them that much. However, it is starting to affect everyone. Sorry, I have to say it.

And I think it's an important subject that everybody speaks about because we can see things changing in the UK and the United States where freedom of speech online specifically is being hampered. And then there's DNS blocking and there's website takedowns in the region that will start to take place in these areas, as we can tell. And then a question to raise on these communities where content is being blocked.

This is very important for progress and how does it affect people and the GDP growth of these countries? I know this is something probably we don't want to talk about at ICANN, but it does affect people. I'm someone who had to circumvent the Internet since I was a kid to get access to specific content to learn, to at some point become part of the SSAC.

So, these are really important conversations. I'm very happy to hear this, and I want to thank the panellists. And Ram, thank you for representing us.

RAM MOHAN

Thank you. I just wanted to say one thing. I had said it in the chat and somebody had said it might be useful to say it into the mic as well, which is that, there is a difference between domain name suspension and DNS blocking. The end results are often different. When a domain name is suspended. The content associated with it is no longer available, right? But when you have DNS blocking, often it doesn't actually touch the actual content, so there are ways often to circumvent it. So, it's just useful to point out that difference.

MICHELE NEYLON

Sorry, just Ram, I have to disagree with you. That's incorrect. If the domain name is suspended, the domain name is not reachable. The content will still be sitting on my servers. You can get to the content using other domains. Have a look at the Pirate Bay, which used about 30 or 40 different domain names.

RAM MOHAN

You are correct, Michele. What I was trying to say was that, if you try to use, if you try to access that domain name using a VPN or another service, you wouldn't be able to get to it. You are correct. Technically speaking, there are other ways to get to that same

content. I was speaking in the scope of that domain name itself and being able to access content via that domain name. If you try to access the content of that domain name and there's DNS blocking, you can get to it in other ways. So, that's what I was trying to explain.

MICHAELA SHAPIRO Thank you so much, guys. I think this just shows that there's more conversations to come. In that case, I think I'll turn to Rafik. Is that right, to close out?

STEPHANIE BORG PSAILA All right, I'm using Rafik's mic just to say a big thank you for the welcome that you showed them, Jalal and Hamzoz. Our work, the CADE project, is to bridge civil society organizations with fora like ICANN, but then, the welcoming, the warm, the openness that you show the civil society organizations that we bring here, that makes a huge difference. So, thank you, Rafik. Thank you to the colleagues here. And we'll continue the conversation on Wednesday. So, reach out to us for more details right after the session. Thank you.

RAFIK DAMAK Thanks, Stephanie, and thanks to everyone who joined us for today. I want to thank Mia Kerep, because she took the lead to organize this session, and we worked together, and we discussed with the SSAC, and then we were with Kate to have this session.

	The most important here, there are a lot of, we learned, I think, a lot from different example and cases, and we hope that we will continue the discussion and see what can be done. At least, hopefully, we build some awareness for today. And with that, I think we can close the session. See you soon.
ANDREA GLANDON	Thank you. You may stop the recording.

[END OF TRANSCRIPTION]