ICANN86 Seville | PF – NextGen@ICANN Presentations (1 of 2)
Tuesday, June 09, 2026 – 11:45 to 13:15 CEST

FERNANDA IUNES: Hello, everyone, and welcome to our first NextGen and ICANN presentation session. Before we begin, I'll hand it over to Siranush for the scripts.

SIRANUSH VARDANYAN: Thank you, Fernanda. Hello and welcome to the NextGen presentation Day 1 session. My name is Siranush Vardanyan, and I am the participation manager for this session. 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 have also posted them in the chat for your reference. During this session, questions will only be read aloud if submitted within the Q&A pod. Interpretation for this session will include English, Spanish, and French. If you would like to speak during this session, please raise your hand in Zoom. When called upon, virtual participants will be given permission to unmute in Zoom. On-site participants will use a physical microphone to speak.

All the questions posted in the Q&A pod will be read aloud during this session, as time permits and when directed by the chair of this

session. Please state your name for the record, the language you will speak if speaking a language other than English, and speak clearly at a moderate pace. And I will now hand it over to Fernanda.

FERNANDA IUNES: Thank you, Siranush. All right, Salsabil, we'll start with you. If you could please begin your presentation.

SALSABIL YAKOUBI: Hello, everyone, my name is Salsabil Yakoubi, and my work focuses on digital governance, inclusion, and people's identities in public systems. This presentation looks at the hidden layer of digital inclusion, whether internet systems can recognize multilingual users through the domain names and email addresses they use. And I use the Mediterranean as a lens because it brings together multilingualism, migration, and reliance on digital tools and services. So the question here is not only who can get online, but who is fully recognized once they are online.

The starting point is personal and simple. What happens when the internet rejects your name? Arabic is my mother tongue, and this example uses my own name in Arabic, and the email address is also in an Arabic script. And so when a valid name or email is rejected because the system assumes Latin characters, exclusion begins at the first field. And this may look like a small technical issue, but in practice, it can block registration, applications, account confirmation, and communication.

The Mediterranean is useful for this question because it concentrates several pressures at once. From script diversity, migration, and dependence on digital systems. Many writing systems are present and historically rooted here, including Arabic, Greek, Hebrew, Syriac, Samaritan, Tifina, Coptic heritage, Armenian, Cyrillic, and Latin scripts with Deltrics. And these are just a few.

And of course, the mobility dimension makes this issue much more urgent. There is no single total number for regular or irregular migration across the Mediterranean. But this scale is visible from two data points or two indicators: one of them being the EU, which registered around 64 million migrants in 2025, and UNHCR recorded irregular arrivals through the Mediterranean for more than 150,000.

So movement across the region often requires urgent interaction with digital systems, from asylum information to education, housing, work, health, and, of course, municipal services. And so the key shift here is from language access to system recognition. A platform can be translated and still exclude users. So the question is not only whether users understand the system, but whether the system can recognize them. A user may read the page, but still be blocked if their email address is rejected, or their name cannot be entered correctly, or their identifier is not processed.

And so, while translation alone is not enough, people do need to act through digital systems because they need to register,

authenticate, receive updates, apply, and communicate. And so when systems do not support people's scripts, users often adapt. One example is Arabizi, where Arabic is written using Latin characters and numbers in digital communication. Here you can see an example of that. This workaround can be creative and practical, but it's not the same as inclusion. It means users carry the burden of intrabability instead of systems being designed to accommodate them.

And so in a migration context, this burden can be especially serious because people may already face uncertainty, urgency, and unequal access to institutional support. Universal Acceptance means that, of course, here, all valid domain names and email addresses should work across systems regardless of script, language, or length. But in practice, a system must accept, validate, store, process, and display valid identifiers.

Failure can happen at any stage. A form may reject the input. A database may fail to store characters correctly. A platform may display the identifiers in a way that users cannot recognize. And the identifiers may be technically valid, but practically unusable. And so this is where inclusion breaks down. But it's also a trust issue. If users cannot recognize the domain name or email displayed to them, they may not know whether the service is legitimate. And so these failures appear in ordinary user journeys. A valid email address may work in one system but fail in another. A browser may reject or misread an internationalized domain name.

And a platform may also display an encoded version instead of actual readable text.

These inconsistencies reduce usability and trust and can create practical risks. For a student, worker, or person moving across borders, this can mean losing access to a portal, missing an appointment, and being unable to complete an application. So small technical failures can become larger institutional barriers. And the evidence shows real progress, but not actual parity. So ICANN's 2025 IDN report shows 151 internationalized top-level domains representing 37 languages across 23 scripts, with root zone support expanding towards 27 scripts.

So the naming layer is becoming more multilingual, but application readiness still lags. UNESCO and ICANN report that only 10% of the top 1,000 websites accept ITNs, and only 22% of global email services under generic top-level domains support local language emails. Also, website testing shows the same gap. So, fully local language email acceptance increased from around 8% to 14%, but that's still far behind the ASCII-based formats.

This is where ICANN's role becomes even clearer. So the domain name system, or DNS, allows people to navigate the internet using names instead of numerical addresses. Internationalized domain names, or IDNs, allow those names to exist in different scripts. Email address internalization, or EAI, extends this logic to email addresses. ICANN account now supports sign up and sign in with internationalized email addresses in local languages and scripts,

and ICANN and UNESCO also support Universal Acceptance Day, curriculum work, and expert guidance.

So the direction is indeed positive, but the challenge is wider adoption across everyday systems. And so the next step is to move from progress to normal practice. First, Universal Acceptance readiness should become a standard requirement in public sector procurement and digital public infrastructure. Second, high-impact systems should be tested regularly, forms, databases, identity systems, email services, and public portals.

And third, technical training should reach the developers, system administrators, universities, and public sector digital teams. And of course, fourth, local initiatives should help communities test the systems they depend on, because the goal is not only to build multilingual identifiers, but it's to make them work reliably where people need them the most.

So the conclusion is simple. A multilingual internet must not only display languages, it must also recognize multilingual users. Universal Acceptance connects technical infrastructure with real-world inclusion, but without recognition, participation remains incomplete. So for ICANN and its community, Universal Acceptance is part of building an internet that remains global, improbable, trusted, and usable across languages, scripts, and communities. So that is it. These are the sources if anyone wants to read more about it. And thank you.

FERNANDA IUNES Thank you, Salsa, for your wonderful presentation. We do have a question in the audience.

BARRY LEIBA Hi, this is Barry Leiba. What is your sense of why we're not already there? What are the barriers to Universal Acceptance that we have to cross?

SALSABIL YAKOUBI Well, I do think that, of course, ICANN has done wonderful work on the naming layer, but it's more the take-up. So I think that what they do, as a coordinating entity, they could support, for example, creating a readiness level, maybe tests. So, actual high-level systems could be used to test how ready they are for Universal Acceptance. Also, for government portals, that's also important to help them, for example, with public procurement of digital systems to choose the systems that are right for them, that are the most inclusive.

FERNANDA IUNES Thank you. Any other questions for Salsabil View? Alfredo, yes, go ahead, please.

ALFREDO CALDERON Thank you for your presentation. It was really interesting. Now, I do have a question for you. Today, we had a session this morning

on Universal Acceptance and different initiatives that are going on. What do you feel or perceive as the impact that Universal Acceptance is having in the new round of ETLDs that has been opened for the underserved communities that would like to apply for a top-level domain, but they can't because of the lack of their scripts that they can use?

SALSABIL YAKOUBI

Yes, of course. I mean, Universal Acceptance has been pushed by ICANN for the past 10 years since there was a working committee. And then, recently, since 2025, change the objective, not just from the actual naming system, but now towards application. So yes, I think ICANN could help provide the necessary training, the necessary knowledge for these local initiatives.

And also, of course, it's a lot to tackle. So I think collaborating and really helping them test what's right and what works for them based on the priorities that the local community prioritizes and what they need. What does that local community -- what are the websites they use?

FERNANDA IUNES

Thank you. We don't have time for questions right now, but if we have time at the end, we can come back. All right. Thank you so much, Salsabil. Wonderful job. And next we have Maria Pericas. Maria, please go ahead.

MARIA PERICÀS RIERA

Thank you so much. So today I'm going to be focusing on the very current question of: Are we heading towards splinternet? The future of internet governance. We're going to try to analyze the current trends and also what ICANN as a community can do about it. So very short about me, I'm currently studying for a master's in politics and technology at the Technical University of Munich. Previously, I was also an early-career fellow with the Internet Society. And also, I worked at a think tank in Berlin on the project Norms in Cyberspace.

So first of all, what is Internet fragmentation? ISOC defines it as the division or splintering of the unified open and global internet that we all know into a smaller, more isolated network subject to different rules, regulations, and technical standards. But this doesn't come from a void. There have been some precedents that brought us to where we are currently. Even if this topic might seem like it came up just a couple of years ago, it was first talked about over 30 years ago when the cyber balkanization term was coined. That was followed a couple of years after with the coining of the concept of splinternet. And then we are all aware of what happened.

So, for example, in China, there was this big expansion of its Great Firewall that was also followed by the Snowden revelations in the early 2010s, that discovered massive surveillance that was disclosed and that led to many countries being more productive with their data sovereignty or digital sovereignty. Also in Russia, a couple of years after this sovereign internet law came into place,

that enabled that Russia would have greater control over their network. And currently, we're facing this US-China tech rivalry accelerating through sanctions, or again, data localization laws, and many platform restrictions. Before going into the details, I would like to do a short disclaimer. As we know, ICANN does not control what happens on the internet, but rather -- I mean, we all know why we're here, right? But still, I think it sets a precedent of the trends that we're seeing, and then we can discuss a little bit more of what we can actually do.

So first of all, we have these internet shutdowns as a very coercive measure of blocking access to the internet. We know it can be, as I just mentioned, through blocking the access to some websites. Also, there's this measure called throttling, which basically means slowing down the broadband so much that it makes it just impossible because it's just so slow that there's no way you're going to have the patience to do that, or a complete cut off.

One of the best-known examples is in Kashmir in India that it had the longest internet shutdown in history. Here we see this young woman holding the paper with "100 days with no internet," but this number raised up to more than 500 days without internet, and it's needless to say what the consequences for both societal but also economical consequences of this are.

Also, it's important to mention the role that firewalls are playing. Of course, the most well-known one is the Chinese Great Firewall that affects over one billion people worldwide. And also, the

problem that I see in this is that it's not only staying in China. Because, for example, there was this research that JIT Networks, which was an organization or a company that was very relevant in the building of the Great Firewall, is now selling these censorship and surveillance technologies abroad in countries such as Myanmar, Pakistan, Kazakhstan, or Ethiopia.

So we see that this trend is expanding and is not staying just in some states, but rather that this is something that could become more and more prevalent. And another way of control is data localization. For example, Russia has been, over the last decade, tightening its internet controls. For example, there's this law already that is 10 years old that makes it mandatory for companies to store personal data on Russian citizens on local servers.

This could be thought of, oh, this is something very interesting. I mean, we are seeing also this trend in Europe of digital sovereignty and so on. The thing is that analysts say that, for example, in the case of Russia, this could mean more governmental access to critical or sensitive data of citizens that would again contribute to the environment of repression of dissidents inside a country.

So why does ICANN matter here? I think we have been seeing attempts of trying to break or trying to diminish this multi-stakeholder approach that the Internet was built on. So, for example, in 2010, there were some China and Russia proposals at ITU that asked to expand the influence of the countries over the internet identifiers. I mean, today I was talking on the bus with

some colleagues from ISOC, and they were telling me that hopefully this is probably not going to happen any point soon. However, we should not forget that there is some intention there from very big, very powerful states.

So, why does ICANN matter? Exactly because ICANN has been clear that the internet should be interoperable, and it has also been advocating that the internet should be based on a multi-stakeholder approach. I just saw yesterday as well that ICANN is going to allocate $1 million for the IGF forum.

Again, one of the key pillars of the multi-stakeholder approach on internet governance. And it's also very important that ICANN prioritizes technical stability over political interests. I was reading about that when the war in Ukraine started, a Ukrainian minister asked to ban or to forbid Russian domains, but ICANN said no, because we are prioritizing this technical stability, and it's also important that Russian citizens have access to information, which is already very restricted. So, this is why ICANN matters. What does it mean for us, and what can we do in our own communities at the local level, national level, or even as a whole of the ICANN community?

One of the most important things that we can do is just stay informed and act in our own fields. Being aware of what is happening, reading the news, and trying to understand how people are being affected by all these types of measures. Because as we

are seeing, fragmentation is real, it's happening, and it has direct implications for millions and millions of people worldwide.

And we also have to be aware of the fact that every policy decision, every technical decision, every technical standard is a chance to make a positive difference in the current environment. Thank you for your attention. I hope you have some questions or feedback. There's also my contact if you also want to discuss some of these topics during some of the coffee breaks. Thank you so much.

FERNANDA IUNES: Great job, Maria. Very interesting topic. Any questions in the audience? Naveed, please. And remember to state your name for the record as well.

NAVEED BIN RAIS: Thank you for your presentation, Maria. My name is Naveed. I'm one of the NextGen mentors. Because you used the words "fragmentation of the Internet" in your title, my understanding of internet fragmentation is the fragmentation of the DNS, not just internet shutdown. So, what is your opinion on the introduction of a parallel DNS architecture that some parts of the world could introduce, and that could fragment the internet? But the on-and-off shutdown of the internet, people would see it from a different angle, because that is not actually a fragmentation of the internet that we use. Thank you.

MARIA PERICÀS RIERA

Thank you so much for your question. And this is also a question I had myself while doing the research, because when I was reading about fragmentation and splinternet, I saw different layers of it. I was seeing that some people were focusing more on the technical one, some more on the governmental one.

So basically, I could see these different layers of fragmentation can be either on the technical level, government, or even commercial if it's done by a big company. And I think also there's a lot of scholarship debate among academics of what it means and what's the exact definition on that. So, yes, thank you for pointing that out. And as I saw, it's also an ongoing debate.

FERNANDA IUNES

Thank you. Any other questions in the audience? Yes, go ahead, please.

PETER JIA WEI CUI

Hello, this is Peter Jia Wei Cui from TWNIC (Taiwan Network Information Center). And my question will be focusing on the political impact and also on the potential blocking of the internet as well. Because, as you can see, those internet blocking cases are basically more from maybe some governments, they have their own political agendas, or they want to fulfill their purpose.

But I mean, I think if you want to figure out these kinds of problems, it's over the rims that ICANN can engage with. Because ICANN is focusing on the domain name systems and the technical era. So I

wonder how you navigate these challenges and issues to prevent the internet from becoming the splitternet. I really like that name.

MARIA PERICÀS RIERA: Yes, exactly. So ICANN, as I mentioned in the presentation, cannot do anything about the Great Firewall or any of them. However, what we can do as a community, not only through ICANN, but also through ISOC, or different organizations that are out there, is advocate for this open internet, through funding or through fellowships like this one. I think they are an opportunity to join efforts, to be aware of what is going on, and for each of us to work on our local levels on trying to be more connected and to advocate for this global open internet that we hopefully will be able to enjoy for many, many more years.

FERNANDA IUNES: Thank you. We have time for one more question. Alfredo, go ahead, please.

ALFREDO CALDERON: I'm Alfredo. I'm also a mentor for the NextGeners. My question for you, Maria, is regarding the role that you as an individual can have to avoid this concept of fragmentation or splinternet.

MARIA PERICÀS RIERA: That's a very interesting one, and it's something that I'm still navigating. Because, of course, as a young person still trying to

figure out how this ecosystem works, the impact that you can have, hopefully, is going to grow over time. But I think it's especially important to work with the people who are facing those challenges in the region. So maybe I, as a person coming from Spain, living in Germany, can try to get in contact with people all over the region, try to better understand, and then advocate.

For example, in the case of Europe, to try to advocate for this not to happen in any other countries, either in Spain or in Germany, or at the EU level. Basically, being a model role or giving an example for other regions, and explaining why this is important. For example, I know that Internet Society, when they try to explain why a country shouldn't block the internet, they try to point out the economic damages that it's doing, saying, "Hey, every single hour that you don't allow internet access, you're losing that much money."

So I think this is interesting to point out. I think also, collaborating with other NextGen fellows. That's always a good one, because I think we're all doing great work in each of our fields, and in the future, I think we're going to have many other points in common to keep collaborating.

FERNANDA IUNES Thank you so much, Maria. Great job answering the questions as well. And next, we have Kristina Ivanova. Kristina, the floor is yours.

KRISTINA IVANOVA

Hello. I would like to present Agentic AI Methods to Support Reasoning and Consensus in Income Policy Deliberations. The core contribution of this work is structured reasoning support. So, for example, we can take a real LGR public comment proceeding, additional reference label generation rules, and related updates, including the updates in Arabic scripts. And in that process, the record is already distributed to different technical and procedural sources. And what I'm proposing is a structured step-by-step human-controlled process in which AI helps analyze material and generate transparent reasoning artifacts.

So the flow is straightforward: the comments go in, the systems then decompose issues and retrieve the evidence, and it produces structured outputs, and finally, of course, humans review everything. And the boundary is crucial, so AI doesn't decide, doesn't vote, and doesn't determine policy outcomes and doesn't replace the people, of course.

The challenge is not just the volume in a huge number of documents, but also the complexity, because in that kind of processing, the community is trying to reason across several kinds of materials at once and interviewing new and updated reference LGRs across several scripts and languages, including Arabic, Japanese, and Latin-related languages. They may need to go across public comments and draft updates, background explanations, and supporting technical materials. And all while understanding how these documents should relate to DNEA's

stability, implementation consistency, and usability. And this creates a real risk.

So important concerns can be missed, ambitions may remain unresolved, and assumptions may stay hidden. And it also slows down the progress because first, people should reconstruct the record before they can evaluate it. In technical proceedings like this one, the input may involve the ICANN organization, technical experts, language communities, public commenters, staff, and participants with different priorities.

So some groups can focus on script accuracy and language representation, others may focus on security and stability implications or implementation feasibility, consistency with existing LTR structures, or alignment with relevant ICANN reference materials. And the key questions become very practical. Who supports what and why? Where exactly does this agreement lie? What remains unclear, inconsistent, or undersolved? And these questions are difficult because they involve a lot of actors with different perspectives. And the same issues can be due to different technical or policy language.

So the methodology, the first system breaks the review into specific technical questions like which LTRs are new, which should be revised, what script or language each change affects, and what change is being proposed. Second, it retrieves the evidence from ICANN materials, sorts it, and organizes the evidence into structural outputs. So, for example, it can show which changes are

being proposed for what language, what justification the ICANN organization provides, which comments support the change, which require clarification, and which are technical or implementation concerns.

Fourth, it checks for gaps and conflicts. It can identify unclear, rational, unresolved variant issues, possible inconsistencies across the LGR sources, and places where the impact of rule change is still underexplained. And fifth, of course, it iterates as new comments arrive or revised versions are updated, outputs also can be updated with source links and change tracking. And the point is to make the review of complex LGR changes more transparent and traceable.

So here's a use case that we can use. And the first one is synthesizing multi-stakeholder feedback. So the input could contain comments, stakeholder statements, and working group drafts. And the output would be a position matrix with citations. And so, for example, we can see that one stakeholder group may express conditional support because public interest safeguards are needed. And the second may express caution because DNS stability risks are undefined. And another may support a proposal because it sees it as a proportionate risk. And it helps participants see agreement and dispute points faster, and it preserves minority views instead of losing them in general summaries.

The second use case identifies gaps and missing technical clarity in draft policy text. So here a system checks for ambiguous or undefined terms, internal contradictions, and unstated

assumptions. So assumptions like who will implement something with what timeline, and with which dependencies, and also a very useful question: if the proposal is adopted, what changes, what breaks, or what else is affected? And the system generates clarification questions and suggested edits, each linked back to the relevant source text. It helps working groups focus discussions, whereas the draft is focused on the least clear or weakest point.

A more realistic approach is a pilot, and the best pilot will be low risk and high value, for example, one public comment proceeding or one working draft cycle. A fixed corpus of documents should be the first selected, and then the system would generate a set of artifacts such as a position matrix, visitations, an open issues list, and a trade-off summary.

And after that, SO/AC participants would review, validate, contest, and correct the outputs, and updated versions could be then published with change logs and source links. And success would be measured by whether this reduced the time of map positions, reduced undersold ambiguities, before consensus calls, and produced traceable outputs. And of course, here, governance is important.

And because AI is used in ICANN policy deliberations, it should be transparent, so every output must be decided and source-linked. And of course reproducibility, because the same inputs should produce traceable outputs, and of course human-in -the-loop and natural facilitation, so the system shouldn't advocate for

reposition. And of course, there are also important risks that should be manageable, like hallucinations, false certainty, biases in summarization, overlines on AI, and privacy exposure in input materials. So the output should be auditable and contestable. I will close it with three takeaways.

So first, ICANN policy faces scale and complexity challenges. And second, agenting AI can help by generating structuring artifacts. And third, none of this should be adopted without human oversight. And overall, the logic is also simple. So documents go in, and agentic workflow, clarity and visibility, and better deliberation. So not better governance by replacing people, but better deliberation by supporting people. And I want to close my section with these practical questions, like which ICANN process could be the best for the pilot, and which output format would be most useful for it? Thank you very much for your attention.

FERNANDA IUNES: Thank you, Kristina. Any questions? Yes, Hugo, go ahead.

HUGO RAMIREZ: Hi, my name is Hugo. Have you looked into a specific policy, or is that part of the future work?

KRISTINA IVANOVA So here's the first example that I provided. It was about label-generating rules with updated Arabic scripts. So I looked at this specific policy for the first example.

FERNANDA IUNES Okay, any other questions? Alfredo, go ahead, please.

ALFREDO CALDERON Alfredo Calderon, again, mentor for the NextGen. My question for you, Kristina, has to deal with the process that we use now in the policy development process. When you mentioned the way you would like it to be handled, do you foresee that the process of implementing the policy will be shorter or not?

KRISTINA IVANOVA I think I'm not fully understanding your question. So you mean if my changes will be really workable?

ALFREDO CALDERON Yes.

KRISTINA IVANOVA I think, yes, because the most important thing is that it's not replacing people, it's not replacing your view. It's just trying to summarize whole facts or internal contradictions that we can have, because we can proceed with a lot of documents. And agentic workflow can help with it because, first of all, it's working not with

whole documents itself. So you can put your documents in chunks. And an AI agentic workflow, if we are working with RAG, augmented generation.

So first of all, we can create the vector embedding and store it in the vector store. And when AI agentic needs to work with an important part of the document, it can take the relevant chunk of the document. It's easier for agentic AI to work with a lot of documents than for people. And then people can see more clearly, for example, the position matrix, all views, all comments, and everything important, and then can decide what they can do with it.

FERNANDA IUNES

All right. We have a couple more minutes here. Any other questions for her before we move on to the next presenter? Anything in Zoom, Siranush? All right. Thank you so much, Kristina. And with that, we'll move on to Aman Ali. Aman, please. The floor is yours.

AMAAN ALI

Good afternoon, everyone. My name is Amaan Ali. I'm a law student at University College London, and I'm genuinely glad to be in this room with people who have spent years dealing with the questions I'm about to raise. And I want to begin with a simple question. What does it mean to be private online? That question, deceptively simple, is at the heart of everything I want to talk about

today. And I believe the answer matters to every person in this room.

In 1982, Elizabeth Fienler at Stanford built WHOIS for a network of a few thousand people. It was a directory, open, frictionless, no questions asked. For three decades, that worked. Cybersecurity enforcement tracked malicious domains. Lawyers went after trademark abuses. Law enforcement had somewhere to start. But the internet grew, and we ended up with 360 million registered domains, and the same openness that helped the researchers, now it helped the stalkers, the spammers, and the data harvesters just as well.

The architecture had not kept pace with the world, and everybody knew it. Then, in May 2018, GDPR arrived. It did not mention WHOIS by name. It did not need to. The conflicts were immediate. WHOIS published names, addresses, and emails indefinitely to anyone with no defined purpose. And that is not data minimization. That is not purpose limitation. That is just everything for everyone forever.

ICANN's 2019 temporary specification was a stopgap. It bought time. A permanent registration data policy finally arrived on the 21st of August 2025. But the story does not end there. So what changed? Privacy became the default. Personal data is no longer publicly visible. The public record now shows only the domain name, the registrar, registration date, and name servers.

And WHOIS, after 43 years, was replaced. On the 28th of January 2025, RDAP became the definitive source for all gTLD registration data. I'm sorry, I'm dropping all the dates. So RDAP was the first protocol designed with tiered access in mind. Different users see different data based on who they are and why they are asking. But here is where we need to be honest. RDRS, the Registration Data Request Service, is not tiered access. It is a form. You submit a request, and a registrar decides whether to respond. There's no defined criteria, no enforceable timeline. And the results show it.

Three numbers that I want you all to keep in mind. 79% of legitimate requests were denied in the first six months, nearly 4 in 5. 41% of the gTLD domain space is not even in the system. Because participation is voluntary. And when a response does come, you have been waiting seven days. While a phishing campaign can compromise thousands of people in under two hours.

RDRS was described as a pilot to measure demand. Fair enough. But a 79% denial rate is not just a data point. It is a signal that the system is failing. So are we protecting privacy? Or are we blocking the very actors the system was designed to serve? That is not a rhetorical question. That is the central design problem of our moment. And while we deal with that question, the EU keeps moving.

In February 2026, the European Data Protection Board and the European Data Protection Supervisor issued a joint opinion on the

digital omnibus package. It directly intersects with domain registration data. The e-privacy regulation is still being negotiated, and ICANN has spent seven years reacting. From the 2019 temporary specification to the registration data policy, reactive, not proactive. The window in Brussels is open, but it will not stay open indefinitely.

I want to name the tension clearly because it gets blurred. Privacy is a fundamental right, and Article 8 of the EU Charter protects it. Doxing and harassment of a domain registrant are documented harms, not hypothetical, and a blogger who registers a domain should not have their home address published for anyone who asks. But accountability matters too. An internet where bad actors cycle through domains faster than investigators can even file a request, that harms trust in a different way, that is not actually a choice between two values. It never was.

The real question is who gets to know what, under what conditions, and why? And the answer is contextual integrity. Privacy is not violated per se by disclosure itself, but by inappropriate disclosure. Information flowing to the wrong context. Medical data shared with your doctor is appropriate. Shared with your employer, it is not. WHOIS treated a journalist investigating a disinformation network and a bulk data harvester identically. IDRS, as it currently operates, still largely does, in a different way. There's no difference in how you are treated based on who you are and what you need the data for.

The solution is what SSAD was trying to build: a tiered model. Tier one is public technical data. Anyone, no authentication. Tier 2, verified users. See the organization name, country, and abuse contact. Tier 3, accredited requesters like IP professionals and security researchers. And Tier 4, the judicial access, court order, full disclosure. And where I come from, open banking and national health services in the United Kingdom already use architectures like this. So, what do we do? Three pillars I want everyone to keep in mind.

First, universal RDRS coverage. 59% participation is a pilot, and ICANN must move from voluntary to mandatory RDRS participation for all accredited registrars. There is no justification for a 41% blind spot. And second, I know there is a supplemental recommendation process that is now underway. It started in May.

In that progress, I believe there should be automatic decisions based on verified identity, not discretionary choices by individual registrars. Identity provider testing is already underway as of May 2026. Build on that infrastructure and make the accreditation layer mandatory. So I will say another one for the second. Urgent request timelines must be separated from standard ones. Seven days for a live phishing attack is not a response time. There is a public comment process on this open right now. It should produce something with teeth.

Third, ICANN needs a permanent seat at the table in Brussels, not to lobby, to co-design. A joint ICANN-IDPB working group

established before the next regulation passes would be a structural achievement that no amount of reactive policy can replicate. This community cannot afford another seven-year cycle. I want to make this clear. Privacy is not the enemy of accountability. Opacity is. The SSAD recommendations were rejected in March because they were not good enough. That honesty matters.

Now what comes next has to actually work. RDAP is technically ready for tiered access, but it lacks the policy. The supplemental recommendation process is the policy window. The IDPB is writing rules right now that will shape this space for years. The challenge in front of this community is to stop building systems that protect privacy on paper while blocking accountability in practice, and build something that earns trust on both sides. That work is happening right now, and that is the challenge, and it belongs to every person in this room. Thank you.

FERNANDA IUNES Great job, Amaan. Any questions for him? Yes, please.

JOHN LEVINE I'm John Levine. I'm an SSAC member. And I must say, I'm delighted to hear this talk. We have spent years with academics coming and saying everything needs to be private and secret, and waving off the security issues. And it's nice to hear a talk that understands that it's an important trade-off and that to the extent

that you don't have the security, you're violating the privacy of the people that the bad guys are victimizing.

And one suggestion I would make is to talk to RIPE. The IP address registry, which is located in the Netherlands, has a similar RDAP for IP addresses. And basically, all of their information is unredacted. So presumably they understand GDPR. The obvious question is, what does RIPE know that ICANN doesn't know? And perhaps ICANN can learn from it.

AMAAN ALI

I think that is a very good point. And the example I gave, how the financial industry and the health industry in the UK, even they follow GDPR. And at the same time, they also understand that this data is very important for security purposes as well. For example, for financial purposes, if we become opaque with that data, no financial fraud can be traced, or no action can be taken. So that is why I think ICANN should be taking the same steps and make it a tiered access where it decides who gets what on the basis of verified individuals.

JOHN LEVINE

Actually, another related thing is that Steve Crocker has been working on something he calls Project Jake, which is a form of tiered access. And he's actually here at this meeting. And if you can

find him, he would be delighted to talk to you about it because he's been thinking about the whole tiered access issue in great detail.

AMAAN ALI

Thank you. I will definitely have a conversation. Thank you so much.

CHARBEL CHBEIR

Hello. First of all, my name is Charbel Chbeir, for the record. I loved your presentation. It's very good and very well-structured. And I have a question for you. You talked about ICANN, WHOIS, and the data privacy and data protection, which is GDPR. It was drafted in 2016. It was ratified in 2018. But before that, we have a gap. You told us about WHOIS. It was incorporated in 1982.

Before that, we had something called Directive Européenne [participant speaking in French]. In 1995, we started to take into consideration privacy and data protection. My main question is, you talked about all the European law, Le Conseil de l'Europe, and you talked about RGPD with GDPR. Now, ICANN is based in the US, in California. How can ICANN implement and enforce something that exists outside the borders of the US?

AMAAN ALI

That is why I mentioned that we need to have a permanent presence in Brussels through working groups. So, for example, I understand ICANN is based in Los Angeles, but GDPR is an extraterritorial law, and it applies to ICANN as well. So ICANN is a

stakeholder when the e-privacy directives are being discussed in Brussels. So all of them are extraterritorial law. It applies to ICANN as well because it has a presence in Europe. So this is how it can become a stakeholder in the process and have a conversation.

FERNANDA IUNES Thank you. Yes, Sebastien, please go ahead.

SEBASTIEN BACHOLLET Sebastien speaking. Thank you for this presentation. In Brussels, there's an ICANN office. So, of course, it's important to say that ICANN needs to be present in Brussels, but they are. And ICANN could say it way better than me, who's a basic user of the internet. It's not a presentation, which is the problem here, but I have difficulty understanding why European ccTLDs have not made all of their data disappear, but just part of it, which was linked to physical people. Because when we talk about private data, it's an issue of personal data, not corporate data. And ICANN went, according to me, way too far in this.

So we're building a system to try and solve a problem that should not have emerged in the first place. The GDPR does not require all data to disappear. No, it only requires that the personal data of physical people be protected, not corporate data. So I have difficulty understanding why, for years, ICANN has been doing something, and then on the other side, European ccTLDs are not

forced to do the same thing. But again, thank you for your presentation.

AMAAN ALI

Thank you so much. That was a great point. I just wanted to mention that, yes, I agree with you. Article 8 of GDPR, it talks about personal data, and it has to be identified to a physical person, to GDPR, to act on. And as far as the corporate data is concerned, that is why I mentioned that opacity is the enemy of accountability and privacy. And it's not the privacy that is stopping ICANN to publish some data. ICANN does publish some data, for example, name registrars and some administrative data as well. But yeah, the point is that it has been opaque for all the other data. And that is what I'm trying to mention, that there is no access to data, even for corporate.

So that is why I said that it makes you stand with Google. Even if you are a blog writer with 30 viewers, and Google, a corporate giant, it acts the same for both of them. So I think that needs to be changed. And that is being discussed right now. As I mentioned, there was a 22-point recommendation that was made. It was rejected in March 2026 because it was not good enough; there was no policy for tiered access to work in that. So that is why I said it can work. It just needs more work for that. Thank you for your point, by the way.

FERNANDA IUNES: Thank you so much. Wonderful job, Amaan. Okay, and then next we have Diana. Diana, the floor is yours.

DIANA KOZLOVSKA: Good afternoon, everyone. And thank you for joining me today. My name is Diana Kozlovska, I'm from Ukraine, and I'm honored to be participating in the NextGen program representing the Kyiv Aviation Institute. Today, I will discuss cyber threats in domain infrastructure, focusing on DNS security and the role of DNSSEC in strengthening trust across the internet.

DNSSEC has existed for many years, and its technical benefits are widely recognized. However, deployment remains uneven across different countries and domain ecosystems. Understanding why this gap exists is important because DNS continues to be one of the core components of internet infrastructure.

DNS is often described as the Internet's address book. Its role is to translate domain names into IP addresses. But the protocol was originally designed when security threats were significantly different from those we face today. As a result, DNS didn't include built-in mechanisms for verifying the authenticity of responses. This design choice helped make DNS scalable and efficient, but it also created opportunities for attackers to manipulate DNS information.

One example of this problem is DNS spoofing, sometimes referred to as cache poisoning. In this type of attack, an attacker attempts

to introduce false DNS information into a resolver's cache. If the resolver accepts the forged response, users may receive incorrect DNS records when they attempt to visit legitimate websites, as they thought before. From the user's perspective, everything may appear normal. The domain name remains unchanged, and the destination may closely resemble the legitimate service. This makes DNS spoofing particularly effective for phishing and credential theft. Also, the attack targets DNS infrastructure; the consequences are usually experienced at the application level, where users interact with websites and online services.

To address these weaknesses, the Internet community developed DNS security extensions, or DNSSEC. DNSSEC introduces cryptographic signatures that allow DNS responses to be verified. Rather than simply accepting information received from DNS servers, validating resolvers can confirm that the response originates from an authoritative source and hasn't been modified. It is important to note that DNSSEC doesn't encrypt DNS traffic. Its purpose is to provide authenticity and integrity rather than confidentiality. Today, DNSSEC is deployed throughout much of the DNS hierarchy, including the root zone. The technology itself is mature and well understood.

However, deployment across registries, registrars, operators, and end users remains inconsistent, which is why adoption continues to be an important topic within the DNS community. The data shown on this slide reflects DNSSEC deployment within country code top-level domains. For this presentation, I collected the

information directly from ccTLD registers by contacting them and requesting data regarding DNSSEC implementation within their domains. This provides a registry-level perspective on DNS adoption and allows us to compare how different national domain ecosystems approach DNS security.

The results show noticeable differences between countries. Some registries have integrated DNSSEC into their operational practices and achieved relatively high deployment levels, while others continue to face technical, financial, or organizational challenges. These differences suggest that successful deployment depends not only on technology but also on policy decisions and stakeholder cooperation.

Ukraine provides an example of how security priorities can influence DNSSEC adoption, as cyber attacks targeting government systems became more frequent during the Ukraine-Russia war, and protecting DNS infrastructure became increasingly important for ensuring the reliability of official online services. In response, DNSSEC requirements were introduced for gov.ua domains. The objective was to reduce the risk of DNS manipulation and improve trust in government communications.

The Ukrainian experience demonstrates how DNS security can become part of a broader cybersecurity strategy rather than remaining solely a technical consideration. When comparing different deployment rates between countries, it becomes clear that technology is only part of the explanation. Countries with a

higher level of adoption often benefit from stronger cooperation between governments, registries, and registrars. DNSSEC implementation is usually treated as part of a broader effort to improve digital infrastructure and cybersecurity.

In contrast, slower deployment is frequently associated with limited resources, competing priorities, or concerns about operational complexity. This doesn't necessarily mean that organizations disagree with the value of DNSSEC. In many cases, the challenge is simply finding the resources and expertise needed to implement and maintain it effectively.

The risks associated with insecure DNS extend beyond individual websites. If DNS information can be manipulated, users may be redirected to fraudulent services, exposed to phishing campaigns, or prevented from reaching legitimate online resources. For public institutions and critical infrastructure operators, these risks can affect the reliability of services that citizens depend upon.

As governments, businesses, and individuals become increasingly dependent on digital services, ensuring the integrity of DNS information becomes an important part of maintaining trust in those services. Despite its benefits, DNSSEC implementation requires ongoing operational effort. Organizations must manage cryptographic keys, monitor configurations, and ensure that updates are performed correctly. Mistakes can lead to service disruptions, which is one reason some operators approach deployment cautiously.

At the same time, many of the remaining challenges are no longer purely technical. The necessary tools and standards already exist. What often determines success is whether organizations have sufficient experience, resources, and long-term commitment to maintain the technology effectively. As a result, discussions about DNSSEC increasingly involve governance and operational planning.

Today, ICANN continues to support DNS security through technical engagement programs: DNSSEC workshops, operator training, capacity building initiatives, and research conducted by the Office of the Chief Technology Officer. One area where progress can be made is reducing operational complexity. As DNSSEC deployment becomes easier through automation and improved tooling, organizations are more likely to implement it successfully.

Another important area is DNSSEC validation. Signed domains provide the greatest benefit when resolvers actively validate DNSSEC signatures, making internet service providers and public DNS operators important participants in the process. Governments can also contribute by incorporating DNS security into broader cybersecurity and digital resilience strategies. Registries, registrars, academics, and members of the ICANN community can also contribute by sharing implementation experience, documenting successful deployments, and supporting organizations that are beginning their DNSSEC journey.

Finally, improving visibility into deployment and validation rates can help identify gaps and provide a clearer understanding of where additional effort can be made. The technical foundations for DNSSEC already exist. Future progress will depend largely on cooperation, operational support, and continued engagement across the multi-stakeholder community. Thank you a lot for the attention, and I'm looking forward to your questions.

FERNANDA IUNES: Great job, Diana. All right, I see some questions in the audience. Yes, please go ahead.

LARS-JOHAN LIMAN: Thank you. My name is Lars-Johan Liman from Netnod in Sweden. We are operators of one of the Root Name server clusters and also a lot of other services. And I was also one of the people who arranged the very first international interoperability test of DNSSEC back in 1999. Thank you very much for this presentation. Supporting and holding out the importance of DNSSEC is very important. I would like to add a few comments.

One in general, which is that DNSSEC is complicated. I will not deny that, and it can lead to spectacular problems when it's not configured correctly. And these are noticed, and these are held out as problems with DNSSEC. What's never done is to hold out DNSSEC the rest of the time, when it protects you from all types of attacks and stuff. So 99.999% of the time, it does its job and

protects you, and once in a while, there is a spectacular problem that is held out and probably seen in the news.

The second thing I would like to say is that there is one way to raise the deployment of DNSSEC on the authoritative side, on the domain holder side, which I didn't hear you mention, and that's the one that I think drove the deployment in Sweden to very high rates, and that is price differentiation.

If you, so to speak, punish, or rather, you turn it around and say you give a benefit to those who sign their zones, you create a financial momentum that makes people sign their zones. If it's cheaper to register a signed zone, you go for that. You make the extra effort to sign your zone, and by doing so, you create security. So, price differentiation is a very simple method that registries can use to increase the level of DNSSEC in their registries. Thank you.

DIANA KOZLOVSKA: Yes, I heard about it. Financial incentives always help to increase the implementation of every technical concept, especially in Sweden.

FERNANDA IUNES: Thank you. I see two more hands. Yes, go ahead, please.

ED VENMORE-ROWLAND: Hello. Thank you for your presentation. Ed Venmore-Rowland, the head of AI cybersecurity policy in the UK government. It's a big

question, but how do you think AI is going to change the cyber threat landscape in the context of your presentation?

DIANA KOZLOVSKA

If talking about AI, it can work on both sides, both on the defense and on the attack of DNSSEC. Because most of the DNSSEC, why it's not implemented? Because it's not configured correctly. So AI can help with the correct configuration of DNSSEC so that blackouts of complete negligibility of information won't happen.

But on the other side, AI can be on the dark side of the DNS implementation problem. Most of the attackers don't have the credibility to attack, for instance, DNS-like infrastructures. They don't have prior knowledge. But due to AI, they can have not so proficient prior knowledge and can receive attacks on the DNSSEC infrastructure. So that's why AI can help and negate the DNSSEC protection on both sites.

FERNANDA IUNES

Thank you. Miriam, please go ahead.

MIRIAM SAPIRO

Thank you very much. I'm Miriam Sapiro, a member of the ICANN board. That was a terrific presentation, as were the others. I really want to commend all of you and the ICANN team for this program, which challenges each and every one of us to think about what we

can do better as a community and as groups within the community. So, thank you. Really, thank you.

My question is, I'm curious whether you have already started perhaps the second phase of your research in terms of really focusing on how we can do a better job on implementation, and whether that's working with the GAC, working with some of our other stakeholder constituencies, to what extent. Have you done research, or might there already be -- I suspect there might be quite a bit of research on who's done well and who's lagging, and what best practices we can encourage so that those that are lagging or reluctant to employ DNSSEC will take another look at this question.

Because the examples you gave about attacks on infrastructure, about the ability, especially with the dramatic growth of AI, to fish and to spoof, they are real-life situations every day, and it's getting worse. So I'd love to hear more about whether you're already embarking on a new phase of your research and whether you might team with some of your colleagues with respect to AI and other aspects, and help us figure out what more we can do to address this important concern. Thank you.

DIANA KOZLOVSKA All right. So, regarding further deployment, for instance, of DNSSEC in ccTLDs, the first thing that, for instance, we have mentioned regarding Sweden is to offer financial incentives for governments to implement DNSSEC. For instance, the rates will be

smaller for them if they have the deployment of DNSSEC. That's the first thing that we can do to improve it.

From what I have read about even my country, what's stimulated the growth of DNSSEC adoption, it's the obligement from the government to deploy DNSSEC to all gov.ua domains due to frequent Russian attacks on our internet infrastructure. Because they invest a lot of money in information war. So that's why we can also give examples to many European governments that we don't need to create extreme situations.

When, for instance, Russians attack our critical infrastructure services, and we have complete blackouts, to start implementing DNS tech for the citizens. Because in Ukraine there are a lot of redirections, yes, I have read, to the illegitimate services right now. So that's why more and more people are starting to implement DNS tech, not only in ccTLD domains.

Yes, so that's why I think that we also need to give this example of our country, of the internet resilience that we cultivate, to other Europeans, so that they need to start also to make and manage their budget to informational protection of their citizens. Because Russians, they don't invest money, for instance, in some generic websites. They invest money in ccTLDs. Yes, in redirecting users to incorrect websites to steal their data and use it for manipulation purposes. So that's the second advice that I can give, just to follow our country.

Because we went through this, we can give a lot of key points from our own experience. And the third thing that I would like to mention is to follow the data breach spending. For instance, in our country, we received a lot of data breaches during Russian attacks, like many viruses, like virus pagers that we had. After which, actually, many domains started incorporating DNSSEC because they understood that if they didn't, they would receive direct consequences. So we also have to demonstrate to the governments that the cost of data breaches is much higher than DNSSEC maintenance. So that's the third key point that I can give here. Thank you for the question.

FERNANDA IUNES Thank you so much. That was wonderful, Diana. Last but not least, we have Omran Adam here. Omran, the floor is yours.

OMRAN ADAM Yes, hello, everyone. My name is Omran Adam, and I am honored to be here at the ICANN86. I'm a NextGen participant, and today I will be speaking about AI, internet access, and peacebuilding. And of course, also focus on how digital governance can support fragile communities.

My main message here is very simple, which is that artificial intelligence can support vulnerable communities, but only and only when the Internet underneath is secure, accessible, multilingual, and, of course, reliable and trusted. For fragile and

conflict-affected communities, digital infrastructure is for communication, education, health, crisis response, and peacebuilding. And I would like to explain very briefly why this is very personal to me.

My background connects several worlds. I'm originally from Sudan and now live in Norway. And of course, my journey through Ukraine, India, Egypt, and some other countries as well, where I study, now, artificial intelligence in Kristiania in Oslo, Norway. I also come from a medical background, and my work has combined AI data science and, of course, peacebuilding. And I am the founder of TechAI, focused on ethical customized AI models systems, and the Dialogue Platform that focuses on dialogue, trust building, inclusion, and communication. So this topic is not only theoretical to me, it is very practical. It comes from seeing both the power of technology and the harm of digital exclusion.

The problem is digital inequality in fragile communities. By fragile communities, I mean places affected by conflict, displacement, weak infrastructure, economic instability, or limited public services. In this context, people may face internet disruption, weak connectivity, misinformation, cyber abuse, limited infrastructure, language barriers, and exclusion from digital services.

I use Sudan and Africa here as examples of a broader reality, not as a political argument. When the internet is unstable, people may lose access to health information, education, humanitarian support, financial services, and reliable communication. Digital

exclusion can then become social, economic, and political exclusion as well.

The statistics on this slide should be read as evidence of a wider access gap that still affects millions of people. And if you see in the slides, the internet accessibility in Europe is 92.2%, while in Africa it's only 35.7%. And most of the countries that have access to the internet are either countries that speak either French, English, or Arabic, while the others are left behind. AI can support communities in very practical ways. It can help with healthcare, education, translation, humanitarian response, crisis communication, early warning systems, misinformation detection, and accessibility for people with a disability or low literacy.

But the key point is this. AI only creates value when people can access it, understand it, and trust it. If a community has weak internet, if tools are available only in dominant languages, or if the digital space is unsafe, then AI will not serve that community properly. So AI is not only a software question. It is connected to infrastructure, governors, inclusion, and digital trust.

The slide shows two possible features for AI. On the left, AI without responsible digital governors can increase misinformation, cyber abuse, bias, exclusion, surveillance, and digital inequality. These risks are especially serious in fragile communities where people may already have limited protection and limited access to reliable information. And on the right, we see a more responsible future. Ethical AI, inclusion, accessibility, secure internet, multilingual

participation, and digital trust. The difference between these features is not only technology. It is governance.

Governance shapes who is included, whose language is supported, how secure systems are, and whether digital tools empower communities or harm them. This is one of the most important slides in my presentation. And I can say that ICANN may not be an AI organization, but ICANN plays an important role in the internet environment that AI depends on.

When people use digital services, they rely on users, devices, local networks, ISPs, the Domain Name System, domain names, and the global intranet ecosystem. The Domain Name System helps people reach websites and services through human-readable names instead of only numbers. This sounds technical, but it has a human impact. If people cannot reliably find and reach digital services, they cannot benefit from those services.

ICANN's work around stable identifiers, DNS coordination, universal acceptance, multilingual internet interoperability, and security helps make global digital communication possible. For fragile our communities. I mean by that that it can support education, health, humanitarian coordination, businesses, civic participation, and connection with the world. This slide shows the relationship between AI and internet governance as layers. At the bottom, we have Internet Infrastructure: DNS routing, access networks, and resilience. Above that, we have Governance and Standards: ICANN, policy, security norms, universal acceptance,

and coordination. And above that, we have AI Systems and Applications, such as translation tools, dialogue tools, early warning, education, and health applications.

And at the top, we have Human Impact, like peacebuilding, health, education, and participation. The message is that the top layer depends on the layers below. If the infrastructure is weak, AI cannot reach people, and if the governance is weak, people may not trust the system.

And now let me just show you what that looks like in real life. In fragile communities, AI translation can help people access information in their own language. Telemedicine can help people reach medicine, medical guidance, when physical services are limited.

Educational tools can support learning during displacement or instability. And dialogue platforms can support communication and trust-building. Misinformation detections can help reduce harmful information. Humanitarian coordination tools can help map services and needs. This is also where my work connects. Through TechAI, I focus on ethical, customized AI systems for local context. Through the Dialog Platform, I focus on communication, dialogue, inclusion, and trust-building.

The lesson is simple: technology should be designed with communities, not only for communities. The future should be accessible, secure, inclusive, ethical, and connected. AI will continue to develop quickly, but its benefits will not automatically

reach everyone. We have to intentionally design systems that include multilingual communities, youth, countries such as in Africa, displaced populations, and people living in fragile contexts.

For me, inclusion means more than access to devices. It means access to names, languages, services, trust, safety, participation, and representation. And representation, of course, in digital governance. Young people also matter here. We are not only users of the internet, we are builders, researchers, founders, organizers, and future policy makers.

First, AI needs a reliable internet infrastructure. Without connectivity, AI cannot reach people meaningfully. And second, digital governance affects inclusion. The way we govern names, access, security, language, and interoperability shapes who can participate online. Third, fragile communities must not be left behind. If new technologies only serve already connected communities, AI may increase inequality instead of reducing it.

And fourth, ethical and accessible technology should be global. Trust, safety, multilingual access, and inclusion should not be luxurious. They should be part of the foundation of digital development. And my main message here is that AI can support peacebuilding and fragile communities only when it is connected to responsible internet governance and inclusive infrastructure.

Thank you very much, and I'm honored to be part of the NextGen. And I would be very happy to continue the conversation about AI,

internet, governance, inclusion, and how digital technologies can support fragile communities. Thank you very much.

FERNANDA IUNES: Thank you, Omran. Really interesting work and great presentation. Any questions for him in the audience? We may have time for one, maybe two. David, go ahead.

DAVID MARGLIN: Hi, thank you for that presentation. David Marglin. So, it sounds great. And in the world you live in, the Nordic model, I would imagine that they're already implementing. I don't see it coming to the United States anytime soon, but who knows? Is there anywhere else in the world where you see your vision already happening? Like, communities developing in the ways that you have appreciated that they probably should?

OMRAN ADAM: Well, if I understood your question correctly, I would say that I could see that developing right now in Africa and in many African countries. Europe is, you know, at the front, I could be able to say. They're doing a tremendous job. But also in the Asia-Pacific regions, they're also doing it. Like India, Malaysia, and so many other countries as well.

DAVID MARGLIN

But any specific places that have implemented or started down this road? Any specific communities, regions, or places that we could look at and say they're already doing this?

OMRAN ADAM

Well, I could be able to say, for example, Central Africa. Like, Sudan, Chad, Central Africa, etc. I am from a tribe called Maba that is both in Chad, Central Africa, Sudan, and that area. Our grandparents, they are completely disconnected from the internet. So they're not able to connect with us on the internet because the internet is not accessible to them. So they're not able to access it. While if you check our parents, for example, you find that they may, because they're multilingual. So they have access to the internet because they speak either English, French, Arabic, or other languages. While I have full access to the internet.

So if you go back a little bit, we find that there is a huge number of people who are completely left behind. And that is why if you check the statistics, you'll be able to see that the people who have access in Africa are only 35%. That is like 35 of 1.7 billion people. That is over 1 billion people in Africa who are completely out of the internet.

FERNANDA IUNES

Thank you so much. And thank you, everyone, for being here. And thank you to our interpreters, as always, and to the tech team as well. Join us again tomorrow, same place, same time, for the

second batch of the NextGen presentation. Thank you, guys, you all did great.

[END OF TRANSCRIPTION]