ICANN84 | AGM – GNSO Accuracy: Can We Have Anonymity and a Secure Internet?
Wednesday, October 29, 2025 – 16:30 to 17:30 IST

ANDREA GLANDON: Hello and welcome to the Accuracy: Can We Have Anonymity and a Secure Internet? 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 antiharassment 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 the session, as time permits and when directed by the chair of the 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.

I will now hand the floor over to NCSG chair Rafik Dammak. You may begin.

RAFIK DAMMAK: Thanks, Andrea. And thanks, everyone, for making it to our session today. The last session of the day, so I hope you are full of energy and ready for the discussion.

We are trying today to discuss about the topic of accuracy. It's not a new topic but something we try to cover in several sessions in the previous interaction. And we have also for today what we can share is the position paper, discussion paper from NCSG where we try to summarize our thoughts about the topic. So we are looking forward to the discussion, and I see we have several of our colleagues and friends from the different groups in ICANN. And so we are looking forward to this.

With that, I will pass the mic to Ken so he can start.

KEN HERMAN: Hi. Thanks, Rafik. My name is Ken Herman. I'm with the Noncommercial Stakeholder Group. I'll be getting us started here on the session on accuracy. As Rafik mentioned, it's a topic that has come up from time to time. Can you go to the next slide, please?

We have this agenda. It's probably a bit more structured than we'll turn out to be in the end, but we do try to put things around. And I've already seen in the chat that the answer to our opening question was, "Yes. Can we go home?" So I suspect that it's not quite so simple and that not everybody may agree on what we're all talking about when it comes to accuracy.

So after a bit of an introduction and a description of the position that NCSG has, the idea is to hear from some of our colleagues from different stakeholder groups and different perspectives. And you see some of them there. Tried to cover things like the security implications, the implementation issues that might come around in order to be able to achieve a level of anonymity which we believe should be there. Perhaps what is ICANN's role, and then just some closing round where we can get some discussion going and some questions. If we can go do the next slide then.

We will have then our introduction. A lot of pressures from the domain name system in terms of how we're going to get registration data and what we're going to do with it, and that's why we're here to talk about it.

I'm going to ask my colleague Farzaneh who is going to give us our position, the NCSG position at ICANN and what we mean by accuracy.

FARZANEH BADIEI: Thank you so much, Ken. Hi, everybody. I'm Farzaneh Badiei. I am a member of the Noncommercial Stakeholder Group and Digital Medusa.

Today if you want to speak and make a comment, first you have to give us a copy of your passport or, the passport preferably, and we will put it in a bin and keep it somewhere really, really safe and then

you can get it at the end of the session. We might as well disclose it to third parties if they ask for it.

No, I'm kidding, obviously. I just wanted to give you a taste of what some jurisdictions are asking from people that want to have an online presence and domain name to do in order to have an online presence.

Digital accountability doesn't need identification. Andrea, do we have the slides there?

So when does accuracy actually become identification? Give us your passport or ID card or you cannot register a domain name. Expanding the definition of accuracy beyond contactability risks excluding users and undermining trust and will have severe human rights impact. There will be overcollection of data and there will be surveillance and censorship risks. If you can go to the next slide and the slide after.

Some of the case studies, they keep asking me but do you know if these troubles and the impact that has affected domain names like Internet users? Well, we do have some case studies. There's China Cybersecurity Law that leads to surveillance. The First Wap investigation which was a very recent linkage of accurate data across systems enabled tracking and repression and it was mainly public data.

And a couple of weeks ago Discord had an incident: 70,000 users' government ID photos exposed after third-party vendor breach

during age verification. That's another problem. If we want to identify domain name registrants, then how are we going to keep their IDs? And I know there are technologies out there that are really good and shiny, but Discord had this problem with a vendor. So there are some risks there. Next slide.

So NCSG's position. For us, accuracy of a domain name registrant means contactability. It means that you can contact the domain name registrant in case of an incident. Because we want as a stakeholder group that advocates and advances registrant's right as well as end user rights we want the domain name registrant to have their domain name and maintain it. And in order to do that they need to be contactable. So accuracy in the realm of ICANN should be about contactability.

Unfortunately, Article 28 of NIS2 has brought much misery to this space because it is a tiered approach but has been interpreted that accuracy means identification, and in some jurisdictions there are requirements for submission of ID. Which I never thought in a million years that Europe would do that to us, but they did.

Identity checks like this will turn ICANN into a global ID authority. There will be no centralized and decentralized. And I'm talking as NCSG and I believe in everything I'm saying. I'm just saying I'm not giving you a position. You can bring forward your position as well.

So what does contactability entail? Email works and monitored by the use. Registrant responds to legitimate issues. Registrar

validates the contact channel functionality. And that's it. Next slide and the next slide.

What is the risk of expanding accuracy? It's not just about privacy. I mean, that's very important. It's about expression. And anonymity protects activists and journalists and vulnerable communities. As we mentioned, stored IDs lead to targeting. And access, many people lack access to government IDs. Next slide now.

How can we address these common concerns? Well, I'm not going to go through this too much because we want to hear from others, but there are ways to do this. There is MLAT. There is also various channels that you can do the good work of security you do. And I talked about Article 28 as well which is about [inaudible] anonymity and content [inaudible] personal data. So if we can go to the second slide to the left, Andrea. I'm just going to be…

Okay, so we want to define accuracy strictly as functional contactability, support registrar-level email validation, maintain due process based data access, apply privacy by design and minimization.

And the final message—that is the last one—contactability, not identification. We want to protect the DNS stability but also protect human rights. And they don't have to go opposite way. Everyone to uphold ICANN's mission limits. And we want to reaffirm that WHOIS and RDAP does not equate with a global ID system.

We will put the position paper in chat. And now I go to Sarah to tell us a little bit about…

SARAH WYLD: Hi. Okay, just give me a minute to share my slides. Thank you. I didn't know it was coming so fast. Is that working? Is it doing it? Yeah, okay. Why are there so many things on my screen?

Hi. Hello, everyone. My name is Sarah Wyld. I am the head of policy and privacy at Tucows. I'm based in Toronto, Canada, and I'm really happy to be here today.

In this context, I am speaking not as the Registrar Stakeholder Group I share for policy, although I think what I'm going to say would align with that. But I am here as "the Cow." Okay. One of them.

Today I'm going to share some thoughts on a topic that has been on our minds for a few years both at home within Tucows and here at ICANN. Looking at why requiring the review of domain owners' ID documents is a bad idea. And a lot of what I'm going to say will echo Farzaneh's intro.

The perspective and information that I share today is drawn from a blog post that we published in late August. So if you want to get a bit more in depth and review the sources that we've referenced, you can check that out. There's a link in the slide deck which I expect will be shared with the meeting info, and I'll paste that in the chat in a little bit.

There has been a lot of discussion within ICANN over the years looking at what processes and policies are in place around registration data accuracy. I am going to level set for a minute, and then we can focus on the more interesting parts.

The first thing to know is that registrars collect a specific set of data from domain owners because ICANN contracts and consensus policies require us to do so. This is separate from what registrars have to collect for legal recordkeeping, tax purposes, etc.

The second thing that we should all know is that registrars validate and verify that data that we collect. Validation means making sure that all the fields are filled in and that they're formatted right. Verification means testing to make sure that the domain owner can actually be contacted at the contact info they provide.

Both of those things are required. Domains cannot even be registered if they don't pass validation. And if the domain owner does not complete the verification, then the domain will be suspended and will not work until the data is verified. And on top of all that if the data changes, then it goes through that same process again to validate and verify the new data.

These measures are effective at ensuring that the data is accurate. And very important in the context of processing personal data, this review is proportionate to the situation.

Now some people think that the existing accuracy measures don't do enough. The robot is overwhelmed. Let's pause and just dig into

that for a moment. They don't do enough to what? To ensure that the data is accurate? To stop DNS abuse? To stop all bad things from happening on the Internet entirely and forever? Those are all different goals, and they are not all reasonable things to expect that we can achieve through processes relating to registration data accuracy.

What we have found is that the existing process works just fine. It ensures that domain owners give us data that lets us enter into a contract with them and works when we need to contact them. That is the purpose for processing this data, and the process achieves those goals.

Going beyond that by checking documents to verify registrant identity might sound like a good way to keep people safe online, to combat at least DNS abuse if not all bad things to ever happen online. But there's not any evidence to show that this would actually promote online safety. Instead, what it would do is restrict who can participate in online discourse and ultimately cause more harm than good.

Checking ID either before the regulation is processed or after DNS abuse happens does not help registrars prevent or mitigate DNS abuse. What it does do is prevent a lot of people from owning domains and open up security, privacy, and equity problems.

And how do we know that checking ID does not help prevent DNS abuse? Years of experience. There are TLDs already out there which require review of government issued ID and they have very high

rates of DNS abuse. And there are lots of TLDs that stick with the ICANN validation and verification processes which have extremely low rates of abuse.

What about after the fact when the abuse has already happened? Well, registrars just don't use governmentally confirmed identity documents in addressing DNS abuse, neither when investigating nor when mitigating.

Instead, we look at other factors including whether the domain is actually being used for DNS abuse. The evidence that the reporter provided. The registration data on file. How old the domain is. The reseller if there is one. What the DNS records point to. She has a lot of arms.

We also have tools that help us review domains for potential abuse, and those tools do not check ID. And it might seem like checking ID would make it easier for law enforcement to find bad actors and hold them accountable. But in reality, cybercriminals are not likely to associate their own ID with the domain that they intend to use for abusive or illegal purposes. It is trivially easy for a bad actor to get a "real ID" that they can use to register bad domains.

There are many factors that affect DNS abuse rates, and there are many tools used to stop DNS abuse. But checking ID is not one of them.

Now that we know that checking ID doesn't really help to prevent or respond to DNS abuse or other bad things happening on the

Internet, let's think a bit about the problems that would be introduced by checking ID.

First up, lots of people in this world do not have a government issued photo ID. My research shows that about 500,000 people in Canada don't have ID and millions more around the world. There are all sorts of reasons why this could be the case. Immigration is a common one, but it could be age related where someone has given up a drivers license and not replaced it with another form of ID.

It could be an issue of documentation that does not match the person's preferred or presented name or other characteristics. These are valid reasons. There's nothing untoward or nefarious happening. And people in those situations have just as much right to participate in the Internet as any of us here in this room.

So requiring review of ID to buy a domain name significantly and disproportionately affects people who are already marginalized in one way or another. And that means that the rest of us lose out on their valuable perspectives.

The next problem to consider is how do we know if the ID is real? I personally run up against this in my life because I do not have a drivers license. I have an Ontario photo ID card, and people think it's fake. Who has a purple ID document? I do. People don't understand that it's valid.

Tucows is primarily a wholesale business. We work with resellers who sell domains and other services directly to customers. We also

have a smaller retail business. And we have a support team that is highly trained in explaining our services and troubleshooting technical issues.

What they're not is experts at knowing all the various types of identification documents issued by all the different governments around the world. I learned that recently. There are a lot. There could, of course, be more than one type of valid ID for each of those countries. And so that is a huge amount of documents to be able to assess, and that's just not what the support team is for.

We could outsource this work to our resellers, but then they would have to become experts on international governmental identification. We could outsource it to a third party, but even vendors who offer exactly this cannot cover all jurisdictions.

We could look at using generative AI, but that brings in all sorts of other concerns including whether the AI's evaluation is reliable. Legal implications about AI decision-making that has an affect on a person. And of course, issues around privacy and the security of the ID being reviewed as well as general concerns about the ethics and the climate impact raised by generative AI.

So determining if an ID doc is real is a real hard thing to do.

That leads to the question of fake documentation. This is not a new problem. Bouncers have been dealing with it for years. But it has gotten easy to spoof even biometric IDs, especially with the AI tools available today.

Domain transactions almost never happen in person. This is not the time that Mike showed up at my office because he worked downstairs and wanted to renew the domain. This is not even like booking a flight where you're passport is scanned and checked against a government database and then your face is compared to the ID before boarding. Instead, for domain registrations ID verification would have to rely on scans or photos of the ID and a picture of the registrant, both of which are easy to fake with generative AI.

Now there is a use case where ID verification happens and that is some ccTLDs. So a ccTLD operator may work with their local government to conduct document verification. But this type of process is not available on a broad enough scale and with fast enough processing to be seamlessly built into the gTLD registration flow. And as we said earlier, checking ID is not a guarantee against DNS abuse even in those ccTLDs that require it.

Domain registration services are global in nature, so solutions for problems that affect all domains need to be global as well. Unfortunately, only governments appear to be in a position to reliably evaluate digital identification and that does not scale.

I'm sorry. I talk a lot. Okay.

We also need to think about the security and privacy implications of any potential solution. As a registrar we need to know who we're entering into a registration contract with, and we need to be able to contact the domain owner. But having to confirm that the name

on the domain matches the ID and the face on the ID matches the face of the person buying the domain puts unreasonable obligations on everyone involved in the process, opens us and the domain owner up to unnecessary risk, and imposes a level of scrutiny that treats every customer as a potential criminal regardless of context.

It also creates a very real security risk. So if we remember the guy making fake documentation a couple slides back, now every domain registrar would have a whole database of real ID documents just waiting for him to try to access it. Registrars would be targeted by hackers without offering any benefit to balance out that risk. And we've seen this type of hack already if anyone here uses Discord.

So all of this leads up to an important question: At what cost? If registrars are reviewing ID documents for each domain owner, the time and effort required to do so would result in significant costs that registrars would have to pass along to our resellers and to registrants. This could double the cost of a .com domain. So in the end, we have a higher cost of entry to being able to fully participate in the free and open Internet and being able to express yourself online.

There are some ccTLDs that already require this type of review. We do work with vendors in those cases, and the costs for those TLDs are correspondingly higher. But if someone doesn't have the ID required to buy the ccTLD they want or they can't afford the higher

price tag, they still have another option. They can register a gTLD. So if ICANN were to make ID review mandatory for gTLDs, this option would disappear.

Looking more broadly than the domain industry, we see that governments around the world have started requiring citizens to show their ID documents in order to access the Internet. Popular websites and services are asking users to present their ID to verify their accounts sometimes because of those government regulations but sometimes in anticipation of them.

This has brought with it the same problems we discussed earlier. Unequal access to the Internet. The use of fake IDs often created by gen AI to get around requirements. Valid IDs being mistakenly flagged as invalid. And security breaches where databases of ID documents are compromised.

So it's worth asking the question: What specific problems does a requirement for domain owners ID solve, and is there any evidence that it would be effective? We have not seen that evidence. What we have seen is that requiring domain owners to show their ID does not improve online safety, but it does bring significant drawbacks.

Limiting participation in the free and open Internet to people with government issued IDs from jurisdictions that make it easy for us to verify those documents goes against that freedom and that openness.

Instead, we should stick to processes that work and that are proportionate to the situation, that achieve our goals without causing security and privacy problems, and that put reasonable barriers in place to stop DNS abuse while letting the majority of Internet users continue to go about their business and live their lives online and offline both. Thank you.

FARZANEH BADIEI: Fantastic. Thank you so much, Sarah. So now I go to Nick from .uk to tell us a little bit of pushback on these arguments maybe. Or no, you don't have to.

NICK WENBAN-SMITH: Thank you very much for having me. I must come to more of these NCSG, get the acronym right, sessions. I think it's a very interesting topic and a fantastic presentation actually, especially Sarah. I'm in awe.

FARZANEH BADIEI: Especially Sarah?

NICK WENBAN-SMITH: Especially Sarah. Not you, Farzaneh. I'm actually only here in order to get my passport back from Farzaneh. And obviously from the U.K. since we're going to leave the European Convention on Human Rights soon I can obviously speak from a sort of safe harbor position on this sort of stuff.

My name is Nick Wenban-Smith. I'm the general counsel for the .uk registry. I also chair the ccTLD's DNS Abuse Standing Committee. And I'm also a data protection officer for my organization.

So I look at it more from, I guess, a U.K. perspective necessarily but also a ccTLD perspective. And I appreciated Sarah's comment like actually we have to do this because we are legally required to. And I think it's very easy to get upset about regulations in different places, but that is the law and you have to do it. And even though we are still in the ECHR anonymity is not a human right as such. So there are competing issues.

I think from my perspective of course you need to be able to contact a domain registrant, particularly in situations where there's a dispute about the domain name. In terms of the intellectual property position or content related issues, you need to be able to reach out to that person and it's difficult to do that if you do not know who they are.

And similarly, the context of it all is very important in the sense that if you know who the person is, if it's an intellectual property situation—I know John is here and can speak to this—but if it's a competitor abusing a trademark in a trademark sense, then that is a useful datapoint in assessing whether or not there's something wrong going on here. The number of people who have said to me, oh, yeah. It's for my art project. I'm thinking, no, it's not. It's selling fake goods.

So that is something. And I think the issue I have I suppose is that where you have abusive domain names there's a very high correlation with provision of inaccurate data. So it's definitely a useful tactic. It's not the solution. I completely agree it's not the solution. But it is a part of the things that are in our armory in order to reduce levels of abuse.

And I will also say one of the final benefits of Brexit is that we are not caught by an Article 28 of NIS2. But yeah, it does affect. We have registrars in the EU and they're going to have to comply with these regulations. And so we want to facilitate that compliance.

So the way that we do this is that, first of all, we do not require ID just to register a domain name in general. But it is used in a proportionate and legitimate way where there's a very high risk of phishing or illegal use or complaints or other things in order to work out whether actually this is a genuine user domain, genuinely registered for legal purposes or not.

And obviously, we do not keep acres and acres and acres of domain registrant ID data. It's done for a very short period of time to validate the contactability and identity of the person who has registered the domain name.

And I guess the final point is that we have terms and conditions for our use of domain names as do most ccTLDs, and that creates a direct relationship between the registrant and the registry. So we are a part of the contractual framework in these sorts of situations

in a way that perhaps with a specific gTLD lens you don't appreciate or one doesn't appreciate.

I think the gTLD scope and landscape, as has been pointed out, is extremely complicated. But for us, we have over 10.2 million domain, 97% of those are registered to people who are U.K. residents. It's pretty easy to get valid identification. We are not prescriptive about that. And if somebody calls us and they do not have a passport or some sort of identity, then we will help them to do cross validation and verification processes if it's needed at all.

So a bit of food for thought. I mean, it's a little bit more complicated I think than just that ID verification and domain name registration completely divorced and should stay that way, I would say. But I would, wouldn't I, so I can get my passport back?

FARZANEH BADIEI: No, I'm sorry but not after all these things you have said. We're keeping your passport. I mean, of course we can change bad laws in a democracy, Nick. We can't just say, oh, a law is a law. No, we use human rights tools and impact assessment tools to see what sort of impact they have had, and we will change them. I mean, I don't know how long more we are going to have a democracy [inaudible].

Okay, thank you so much for this. But of course, your perspective is more from the ccTLD perspective, which is very different. So you're not saying that ICANN should become an ID verifier and a

centralized system for ID verification or require domain name registrants to verify their identification.

NICK WENBAN-SMITH: Um, I guess that's not for me to tell ICANN anything. I can see some advantages and I can see some disadvantages.

FARZANEH BADIEI: Okay, great, thank you. And also, anonymity definitely is a tool for asserting and exercising our human rights and will remain like that.

[inaudible] can I do a shout? Can you tell us from the law enforcement perspective what you think? Do you want my ID?

UNIDENTIFIED MALE: Yes, thank you. [inaudible] from [inaudible] police here. And I agree with Nick. Anonymity was never a human right. It's just a tool for your privacy. And when in your life you were anonymous? People start thinking because they are going online and they encounter anonymity for the first time that it is a human right, didn't we?

I wanted to comment I keep hearing the word "contract"—contract with my clients, etc.—and when have you ever signed a real contract without verifying your identity like in real life? So I don't think it's a contract, what you are talking about.

And one last thing is this about contactability, of course, we cannot demand everybody to provide their identity and keep copies of identities. But we really need contactability to lead to

accountability. Like if we need to investigate something as law enforcement, we have to, for example, if you give a phone number, we need this phone number to be the phone number of the user of the owner of the domain not just a random phone number or a disposable email address that you only use to verify [inaudible] the domain, etc. So we need to keep a balance of accountability and further investigation if there is need.

Last, I would like comment as the last comment that law always respects your rights and protects your privacy. For example, there is GDPR that messed everything up. It was about the human right of privacy. So you have to trust laws and that companies will protect your data instead of just trying to hide behind anonymity and be afraid of giving your identity.

For example, a week ago everybody arrived here and a kind of ID was checked at the entrance to give you your badge, but you did not complain about that.

FARZANEH BADIEI: Thank you, [inaudible]. Did you just mention accuracy means contactability?

UNIDENTIFIED MALE: No, I said that contactability should result to accountability. For example, if you give a phone number or an email to verify your registration, I would be very happy if when I need to investigate, this email leads me to the real person that's behind the domain. So

you have another layer of privacy in between. of course you will not give, for example, your home address or your passport. But if you give your real email, it's another level of privacy between you and the registrar. But law enforcement needs to be able to trace illegal activity and bad actors to the real person.

FARZANEH BADIEI: Yeah, but I also think that we need to think about alternatives. You might not need to have access to their phone number or their ID. You can verify it in other ways.

But Sarah has her hand up. Yeah?

SARAH WYLD: Thank you. Two thoughts. We regards to what contract are we talking about? I was referring separately to two contracts. One of them is the Registrar Accreditation Agreement which a registrar has to sign in order to operate. And I don't have details as to whether ID is checked as part of that process because that's something that happens on a business level. They were already accredited when I showed up. But the domain owner enters into a registration agreement with the registrar, and that is also considered a type of contract. For that, we do not need the ID.

Second question, you had mentioned the GDPR, and I think what we're discussing here is exactly how these companies comply with the GDPR. How do we implement the privacy law to make sure that we can meet our ICANN obligations, prevent to what extent we can

and certainly mitigate DNS abuse while maintaining our privacy obligations under the GDPR and other international privacy laws like, my favorite, PIPEDA. thank you.

FARZANEH BADIEI: Okay, so I see that we have three people in the queue, and two of them are registrars. So I'm going to go to John first. John, where is John from IPC? Yeah, John, tell us [inaudible].

JOHN MCELWAINE: I certainly agree with Nick and the gentleman over there. We think that having validated, accurate information is crucial. I'm not going so far as to say that we need to be checking IDs, but having some form of the mechanism to validate the data is very, very useful. Obviously, anecdotally speaking when I'm dealing with phishing scams, things like that, I would say that zero percent of the time is it accurate information. So there is some correlation, and I think that even the registrars are seeing that if there was some validation, some other additional hurdles, then there's going to be less DNS abuse going on, less malicious actions going on.

And then I was going to put a question in, Farzi, to you. In terms of contactability if that concept means just having an email address or a Telegram handle or a WhatsApp handle, you can imagine what that could do to allowing criminals to have essentially free reign. So just having a working email address or a way to contact somebody without knowing who is really behind that would really

threaten, I think, the stability of the Internet because it could allow for such easy fake websites, scams, phishing, etc.

But again, I think that having a system that scales and maybe to Nick's point you can identify more high-risk domain names, have a check on that would be a good idea. Thanks.

FARZANEH BADIEI: Thank you, John. I think Sarah in her presentation showed that verifying ID does not necessarily lead to accountability, holding people accountable for their crime. And I believe that the damage and the violation of human rights that can happen as a result of verifying ID outweighs its benefit because we have been mitigating DNS abuse for so long without asking a domain name registrant their ID.

And I do not agree with the narrative that DNS abuse is so bad that it's not well managed. If everyone of us was just coming across bad domain names and phishing and all that three times a day, yes, I would have agreed. But this anecdotal and I am just saying it. But it's still from the study that I also see the methodologies on the increasing DNS abuse and stuff is a little bit flawed, I dare to say.

Okay, so I have Volker here. Yeah, go ahead, Volker.

VOLKER GREIMANN: Thank you. Volker Greimann, CentralNIC. I've been on the front lines of DNS abuse on the registrar side, i.e., defending against, for almost 15 years now. And from experience, I can say with almost

99% accuracy it will not help. No matter the levels of ID verifications we implement it will not make a difference against abuse of domain names.

When we introduced the verification requirement from the 2013 RAA, this led to perfectly accurate WHOIS data. From somebody else. Stolen from a telephone book. We had cases where people tried to socially engineer domain name away from us to get access to an account where we had in the end three copies of an ID document with different signatures, different birthdates, different photographs all of the same person. We couldn't discern which one was the real one.

We had cases where Chinese cybercriminals used the ID documents of students living in Chinese university dorms that had been collected for some purpose that were then being used to register domain names for fraudulent purposes.

We have no ability as an industry to, even if we have 100% verified, certified ID, to identify whether this ID actually belongs to the person that is coming to us. We have no ability as an industry to verify what the purpose and a domain name is going to be used for when it's being registered.

There are patterns that we can use that are not dependent on ID that are very efficient, but ultimately collecting ID, in my belief, or extending the requirements for verification [inaudible] personal data will lead to more harm than good because cybercriminals are

creative. They are the ones that are able to circumvent those procedures that we put in place to as the first line.

What we will be doing if we sharpen our tools and make more requirements and make it more difficult to register a domain name is to cut out legitimate registrants. To make it more difficult to get a domain name. To make the registration workflow so onerous eligible interested parties that they will just say, okay, let's keep my Facebook account.

FARZANEH BADIEI: Okay, so I have Michaela. Okay, Michele and then Michael and then Maciek.

MICHELE NEYLON: Thanks, Farzaneh. I think this is one of these really contentious debates which is why the room is so full. And why the put us in this room is a mystery to me. I think I do like this idea of accountability. I think that's something that resonates with me. But the conflation of domain registration data with ID, with it becoming a proxy for some kind of government ID is very, very disturbing and it's something that has come up time and time again over the past few decades.

Ultimately, we as a company, our business is hosting. Domains are something that also happens to be there. But more often than not it's not just the domain name we're selling to somebody. We sign

contracts with clients of all shapes and sizes who spend anything from €5 a year up to several hundred thousand euros a year.

I generally don't go asking for ID for the people I'm doing business with. If I can't trust the person we've negotiated a contract with is actually acting in good faith, I'm probably going to start having problems in other areas of my business. But that's a whole other conversation.

The accountability piece though I think that's fine. I mean, you can reach the person that's behind the website. The person that's behind the domain. Behind whatever it is, that online resource. And in often cases, it's not the domain name that you really care about. It's probably something else. It's probably some content that's sitting on a server somewhere. Or somebody who has done something from using some kind of online service.

Forcing companies such as ourselves to collect more personal data, be that photo ID or anything else, is a very slippery slope and it's one that opens up a whole other can of worms. One of the most recent incidents we dealt with involved a highly sophisticated, highly targeted attack against one of our clients where the criminals managed to infiltrate the Google accounts of the client. They managed to get into their telephone account. They managed to get themselves onto their telephone app, and they managed to replace the SIM card of the primary phone number in order to basically do…like it's a man-in-the-middle attack by SMS, essentially. So they had access to absolutely every single thing and

were then able to go off and hijack domains, hijack documents, do all sorts of fascinating things.

FARZANEH BADIEI: Michele, we only have ten minutes.

MICHELE NEYLON: Sorry. But the thing is a lot of things do not necessarily involve us as domain registrars or registries. And I think asking for more IDs doesn't help because often these attacks are so complex. I mean, we want help from you all to not have to deal with them. I just think it's something that some people are fixating on the wrong thing.

FARZANEH BADIEI: Okay, great. So I have Michael. And then I see Maciek also. Wow, you got…okay, great. So, Michael, Maciek, and then Rieke. But we should be short because we only have ten minutes.

[MICHAEL]: So, Sarah, your opinion is that ICANN's current definition of ICANN, it's proper, it's working. I don't share that opinion, and I guess my question to you is: Do you think that the majority of the GAC in the public sector working group agree with your opinion or my opinion of that?

SARAH WYLD: I don't have information about the GAC's overall opinion on this topic or how that would break down on a person-by-person basis. I don't count that.

[MICHAEL]: Okay, so I guess a follow-up question is everyone in this room here in order to show up and pick up this badge had to show a government ID. Was that so onerous for everybody? And again, the reason I think that this is important that, Farzaneh, your definition of accuracy just relies on contactability and as you stated, or the paper that's being put forward.

And at the very top of this discussion you talked about how that is inconsistent with certain national laws. Now ICANN's article of incorporation upon which the bylaws rest states the following: "The corporation shall as part of its purposes lessen the burdens of government." So do you think it is prudent for ICANN work or the ICANN community to advocate positions that clearly are creating a burden for governments?

FARZANEH BADIEI: Actually, Article 28, the only requirement is not ID verification. It also gives the different jurisdictions the option to do accuracy in other ways. So it's not going against a law if we define it as contactability. We did not come up with this definition. It's actually when we were talking about [and doing] EPDPs on registration data policy, it's what like the registration data policy is collected to be

able to contact the registrant. It was never about identification of registrant.

So I see Rieke, and Rieke had actually a lot of expertise in Article 28. And I will come back to you, [Maciek. But I want Rieke to—is Rieke in the room? Yeah, okay.

RIEKE POPPE: Hi, everyone. My name is Rieke. I am from one.com which is a registrar in Denmark. I think I love your presentation, Sarah, and I totally personally agree with both you and Volker. And you also made a nice definition of what identification is.

Unfortunately, it's just not true. So in my country, NIS2 has already been transposed. It came into effect on 1 July. And a secondary law is coming in effect as of January which specifies how we're supposed to verify our registrants. And I just wanted to read out there are three definitions of verification in the Danish law.

One is a syntactical verification, and that is what you call validation. And then there's operational verification which is the contactability. And the third one is identity verification, and it is defined in the law as, "The collection and validation of information about a registrant to ensure that the registrant is who they claim to be."

So I don't think that we're talking about collection of ID documents. And also, by the way, we are deleting those once we have verified people just to…yeah. I think we're asking the wrong question.

So my company both has a gTLD registry, a registrar, and a lot of other stuff. So what we should be asking is this verification is already happening in the gTLD space too, and I think it's creating an unequal playing field amongst registrars. Because all of the [one.com] registrants will soon have to verify themselves in a much harder way than any other gTLD around this table. And what are we going to do about that is the question. Not if we're supposed to be an ID verification mechanism. I don't think we should be, but it's already here. And how are we going to handle that is the right question.

FARZANEH BADIEI: So I have Maciek in the queue yet. Go ahead, Maciek.

MACIEK PIASECKI: Okay, I have got many remarks, but I'm going to focus on the most relevant ones. Much of this Maciek Piasecki, and ICANN Fellow, first time. To answer your remark about us showing our IDs to get here, well, as far as I know my ID is still in my pocket here and not on some server that will eventually get hacked and somebody will use this ID to register a fraudulent website to do some DNS abuse.

But I want to ask about the business implications of this regulation. Because we are imposing on the businesses the need to store data which is very vulnerable. And if those businesses are operating in the EU or within countries or states that have GDPR compliant regulations, then as far as I understand it puts their business risk

through the roof because they either need to store this information on their servers that will get hacked eventually or they need to choose a subcontractor in a way that they will need to present to the court that they took their due diligence to protect the data. Thank you. But yeah, that's a question for the business people.

FARZANEH BADIEI: Okay, I don't think we have time. You can talk to them offline, but let's go to Luke. And then Sebastien wants to respond to Rieke, right?

[LUKE]: [Bob Golding Company] borrowing Luke [inaudible]'s identification, and I will be brief. The issue of contact and contract is very important. Everybody in this room makes hundreds of contracts all the time. I don't think there will be anybody here who hasn't bought a coffee, and that is a contract.

Contract should be between registrar and registrant. It should not automatically come with an assumption of criminality. It should not be used to unnecessarily categorize registrants. It should not be used to push an authority controlled mechanism, but it will get used to abuse yet more people. Those people being the registrants we should be protecting through censure and other activities. If you don't take the ID, you can't leak the ID. And if you do take the ID, you will leak the ID.

FARZANEH BADIEI: Thank you very much. Sebastian and Sarah.

[SEBASTIAN]: Just a simple point here. If you do business in the U.K., you should obey U.K. law. If you do business in Denmark, you should obey Danish law. What we're proposing here or what we're discussing is for ICANN to become that law. That is not the role. If you choose to do your business and you were born in Denmark so you didn't, you know, it happened with it, for that that's the way it happens. Nobody's questioning that. What we're questioning is leveling ICANN to that sort of level.

And when ICANN adopted GDPR, it was to allow ICANN's quite invasive position on WHOIS, publishing the whole information online, and bringing it back. Because we were breaking laws. There were too many of us breaking laws in Europe. Adopting a position where we're all grabbing IDs because that's what you do in Denmark is probably going a bit too far.

FARZANEH BADIEI: Okay, great. Thank you. Going back to Michael's earlier comments, we should recognize our privilege. I have a Canadian passport that cost me $150. Some people don't have food. How much did it cost you to get here? Not everyone has that access.

So I think we need to advocate for data driven decisions that do help to combat abuse and do not adversely affect people's privacy rates and their security. Thank you.

FARZANEH BADIEI: Great. We only have two minutes. If you can do it in 30 seconds.

[MICHAEL]: On the clock. Go. I'm here speaking in an individual capacity. I have an opinion no one's paying me to say here. I've been in ICANN for 26 years. This topic has not gone away. It continues to get kicked down the road. Let's go back to the articles of incorporation. It's about lessening the burden of governments.

FARZANEH BADIEI: Great. So, Rafik, do you want to close this now? We are going to continue this conversation and we are going to work on our positions and also we will probably get a bigger room, because you really love this topic, next time.

RAFIK DAMMAK: Okay, thanks, Farzaneh. And thanks, everyone, for this lively discussion. I guess we will have more in Mumbai, so we'll see if we need to do some follow up.

And with that, thanks everyone and see you soon. We're going to close the meeting.

[END OF TRANSCRIPTION]