ICANN86 Seville | PF – GNSO: NCSG Wrap-Up Session
Thursday, June 11, 2026 – 16:30 to 18:00 CEST

ANDREA GLANDON

Hello, and welcome to the NCSG HRIA session, Safeguards and Remedies in DNS Abuse Policies and Beyond. Please note that this session is being recorded and is governed by the ICANN Expected Standards of Behavior, the ICANN Community Anti-Harassment Policy, and the ICANN Community Participant Code of Conduct concerning statements of interest. Please observe the following guidelines to participate in this session. I will also post them in the chat for your reference. Only questions posted in the Zoom chat identified as a question will be read aloud during this session, as time permits, and when directed by the chair of this session. If you wish to speak, please raise your hand in Zoom or 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 for everyone for making it for the last session of the day and of the ICANN meeting. And sorry for the possible confusion since the title and the schedule don't match what we will have today, which is about the human rights impact assessment, and that will be about the authentication and authorization part. So just as quick background, we want for each

ICANN meeting to have this regular session about human rights impact assessment, and to keep talking in a concrete manner, to share examples, to go on a real case for policy, and to hear from the different parts of the community. So you will expect in the next meeting, and so on, to have a session about human rights impact assessment. And with that, I will pass to Farzaneh Badii, who will introduce the topic and explain about what we selected for today as a discussion issue. Yeah. Farzaneh, over to you.

FARZANEH BADII

Hello, everybody. Welcome. Sorry, we had some logistical issues yesterday. The session was conflicting with the Standardized System for Access and Disclosure. It's not a working group, it's a Supplemental Review Team, and that group is very important to us, so conflicting this session with that required us to move this session to today. But we are just going to have a conversation of what the potential human rights impacts are if we get this authentication and authorization of law enforcement wrong in this space. So it's just a conversation. We are going to discuss the NCSG point of view, and of course, you can weigh in. So just to mention, I'm being a little bit cryptic. By access to domain name registrant private data, we actually mean the data that is in WHOIS, and has been redacted, and law enforcement needs access to that data. And ICANN has decided to come up, well, in the EPDP, there was an accreditation mechanism, but that turned out to be too expensive. So we had the RDRS pilot project for two years, and as a result of that, we decided that coming up with some kind of authentication

mechanism for law enforcement that in the future can be applied to other users as well would be a way to go. So, next slide, Andrea.

What is the problem here? So basically, law enforcement agencies sometimes, in the process of their investigation, need to have access to the domain name registrant private sensitive data. But we call this data sometimes subscriber data, because it's their name, email address, mailing address, phone number. And because there is jurisdictional fragmentation, and sometimes one case can span the victim, registrar, and reseller across three countries, we need a mechanism for law enforcement to be able to request the disclosure of this data. What are the human rights at risk? The basic subscriber data, as I mentioned, can trigger investigations that, in some cases, can lead to deportation, prosecution, death threats, and other issues. Next slide.

So now, these are two interesting concepts that we need to be very knowledgeable about, and this differentiation between authentication and authorization. So, when we talk about authentication, we mean that we need to authenticate the law enforcement agencies to verify officer identity via official government domain email, but also their badge or other stuff that we need. Independent callback to publicly listed agency phone, we should be able to authenticate. And these authentication elements that I'm talking about, these are not what the SRT, the Supplemental Review Team, is talking about. This is what we are saying should be in there. So authentication, for us, is a very important stage because authentication creates some sort of trust

in the registrar, and it might not incentivize them to do more fundamental rights balancing, even if we tell them that they don't have to disclose the data and they should consider human rights before disclosing the data. So at the authentication level, we want to generate that basic trust in the registrar that this is who the law enforcement is. The law enforcement also has the mandate, legislative mandate preferably, to have access to people's private sensitive data. And it can be portal-based verification. There are other products out there, like Google LERS, that are specific for that. It's a proprietary system that's for Google. But Kodex is a third-party authentication mechanism. And also, we want to emphasize the zero trust basis, that you always have to validate and all that. But we should also consider that even verified identity does not equate with legitimate request. And we should be very clear on that from the start.

So now we authenticate the law enforcement agencies, and then they use whatever we provide for them to authorize the request. Now, I see that the title is, so is the request legally valid, and what's the human rights impact assessment? So these are the two important things for us. However, if it's legally valid, that's a question that it could be legally valid in some countries, but the law could be a human rights-violating law. And this is a very important stage, that we need to have certain elements in place. For example, is there a subpoena? So to help the registrar to decide whether to disclose or not. Is there a subpoena? Is there a court order? Is there a search warrant for content data? And also to incentivize the

registrar to do a fundamental rights balancing, we would like to make this mandatory, and we would like to make it jurisdiction agnostic. It doesn't matter whether the registrar is in the EU or anywhere else, they should do this fundamental rights balancing anyway. And next slide. And if you have any questions or if you have any points to make, you can just raise your hand or tell me here.

So what are the human rights that are at risk if things go wrong? Privacy. Subscriber data enables profiling, surveillance, and targeted persecution without judicial review. Freedom of expression. Unmasking the person behind the domain or social media account can silence dissent, journalism, and whistleblowers globally. Free association. Registration data reveals organizational affiliations; disclosure maps networks of activists, minorities, and opposition groups. So we can't buy this argument that this is just their name and their affiliation and just minimum subscriber data. This data, especially now that on the Internet there are many tools to have access to other data, people can be easily profiled. And then life and security. Data disclosed to jurisdictions using the death penalty, where torture is practiced, can have irreversible fatal consequences, and sometimes even in jurisdictions that don't have those, it can be abused and can have implications. Next slide.

Now, one of the concerns that we have, and the community here is a little bit confused about what our concern is, is that when you have the emergency urgent request requirement, it requires the registrar to disclose domain name registrant private information in urgent situations. For example, then the registrar might not, within

a very limited time, for example, eight hours or 24 hours, is that ICANN's? ICANN's 24 hours? So when you have an authentication mechanism in place and the registrar might just think, "Okay, this is an urgent claim from an authenticated law enforcement," they might not be incentivized to do a human rights check, and then as a result, they could just disclose the data, and then there will be consequences for the target: arrest, prosecution, deportation, potentially irreversible. And actually, another concern that we have is that these, first of all, we actually believe that authentication for law enforcement is needed for data protection principles, and we have been advocating for it. But we believe that it should be done very carefully, and there is a risk of getting hacked. For example, these are rich people that get hacked. They are not some under-resourced organizations. So for example, Kodex at some point was hacked, and LERS was hacked, and in some of the cases it was an urgent request. And the FBI last year actually issued a warning that there are impersonators of law enforcement agencies saying that they are FBI and submitting urgent requests and getting access to, this is the FBI's own warning. And so we have a problem here that if in these situations they get hacked, and then the private data is disclosed, then that fundamental rights balancing is not done, and it might end up in the hands of illegitimate. No. Stephanie is asking if contracted parties actually think email from a government domain is good enough. No, and they have been saying that, Stephanie, that domain name verification is not good because it can get spoofed and hacked easily. So we need authentication and in a secure manner. We were chatting with SSAC yesterday about

this, and we were wondering if we could do some kind of security specifications as well that could help with making the system more secure. But I would also like to see more safeguards and maybe remedy for the domain name registrant if this thing happens, if it gets hacked, if the system gets hacked. But that's another, I don't know if we can do this in this Supplemental Review Team, unfortunately. Maciej, do you have a, hey, I know I pronounce your name wrong, but in your public comment, actually about the implementation of urgent requests, you had a really interesting case of a parliament. There were protests in the parliament, if I'm not mistaken. Could you go over that? They could have access to the protesters' data, arguing, so it was about critical infrastructure, claims that critical infrastructure is being attacked, so they have access. Yeah, go ahead.

MACIEJ PIASECKI

Maciej Piasecki, EURALO and ALAC in Spain, also a victim of police repressions, as acknowledged by a Polish court. I personally see numerous risks involved in this process, especially to users, whether they are individual ones or micro and small businesses. So in addition to the narrative of human rights, I think you could consider other freedoms, such as the freedom to do business, as expressed in the European Charter of Fundamental Rights, because there might be more at stake here. As we know, in jurisdictions where there are higher levels of corruption, police can be pressured, or other enforcement agencies can be pressured into using these kinds of powers to either execute surveillance over

political opposition or thwart business competition that's competitive towards entities close to the state somehow. As in, there's a local politician that has a cousin, this cousin has a company, and this company wants to destroy competition. So there might be more than what you have identified here, and as other constituencies are expressing the need to take human rights into the wider perspective, I think that could be relevant.

And as to my public comment, I expressed that in the current state of the documents regarding disclosure of this information, the language is quite foggy, especially the expressions regarding imminent threat to, I think critical infrastructure is mentioned. Critical infrastructure in Polish law is defined only roughly, and the exact definition is under a clause of higher secrecy. I'm not sure what the exact term in English is. And this could pose a serious threat to legitimate users who just don't know whether conducting a protest on a bridge or near a railway station, because that could be considered critical strategic infrastructure, is or is not an imminent threat to it. Whether blocking an airport, which we have seen in Europe in the name of climate justice movements, whether that could make this request legitimate. So in various jurisdictions, even those where police are held to high standards and scrutiny, this could generate confusion and possible risks to both users and public institutions, which will later be challenged in courts.

FARZANEH BADII

Thank you very much. So, this is a case that we raised during the SRT, and we would like to see some kind of clarification. Because at this stage, we cannot change policy anymore because it has been implemented, so that language is in the contract. But what we can do is come up with interpretation and maybe implementation guidelines on how we can clarify the definition so that it can be narrow, and so that the registrar does not just disclose the information when they see that critical infrastructure is at stake. Yeah, go ahead, Andrew.

ANDREW CAMPLING

Hi. Andrew Campling, for the record. Two comments, really. I think, firstly, a really important one. We've sort of focused on the rights of the registrant. It doesn't say on the slide, but I know it has been discussed, this is meant to be a balanced assessment, so this should also absolutely include a rights assessment of the alleged victims. Because otherwise, there's no point doing a rights assessment if you don't do a balanced assessment. So it has to include the rights of the alleged victims, not just of the registrant, otherwise it's completely pointless. Obviously, no issues with the authentication. That's essential. The comment in the chat, though, I noted, made me smile because, rightly, we shouldn't just rely on it coming from a government domain, an email, thinking that that's sufficient. But of course, we do separately seem to be happy to rely on email verification for registrant data. But I think the key thing is

it should be a balanced human rights assessment, not just one-sided. Thank you.

FARZANEH BADII: So that's because domain name registrants are not cops. So cops have a power to prosecute people and also abuse their powers. But the balancing rights, we have been consistently arguing for that, and the human rights impact assessment always has balancing rights in it. Yeah. I'm going to go through how we are going to do the human rights impact assessment, but also if you look at our comments in SRT, you will see that we are for having balancing rights as well. So let's go to the next slide. Oh, I'm sorry, Sebastien. Go ahead.

SEBASTIEN DUCOS: So, Sebastien Ducos from Unstoppable Domains, which is a registrar.

FARZANEH BADII: Yes.

SEBASTIEN DUCOS: A small registrar with a sliver of the view. But until six months ago, I was part of GoDaddy, which is a slightly bigger registrar. It has a significant portion of the market. And at GoDaddy, we didn't have a flag for urgent requests in our ticketing system. But we conducted a study of millions of tickets, not all requests, in conversation with

ICANN, who was trying to gauge the size of the issue, and found, over the last five years, four items that could have qualified as urgent requests weren't even flagged by law enforcement as urgent requests. So we're spending an inordinate amount of time on this, and I understand that policy has to do this, but we need to be very realistic that it's an almost nonexistent case here. What exists is law enforcement requests. There are many. And as I now am looking at this at Unstoppable Domains, and under strenuous pressure from the NCSG, I have decided to conduct a study of law enforcement requests and have a transparency report, which I should have at some point in July. I'm waiting for the first six months of the year. And there's not a huge amount of traffic on a million domains, let's be honest.

But there, and to your point, Andrew, I have to say that it's actually impossible. It would be impossible for me to do that balancing test of the victim, as you say, because when I get law enforcement requests from the US, from India, from other places, regardless of the way I answer, I get a request for data. They're not disclosing what the problem is behind, because it's a police case, and usually that information is not there. So the only balancing test that I can do, if only because of the information that I have, is the balancing test of the registrant. Other requests, when they come from IP lawyers and other entities, will talk about the victims there. I can study. But in the case of law enforcement, that is not the case. There's no information that I have in pretty much all the jurisdictions I've seen. Then to the point that you were making,

Farzaneh, and Maciej also, I have a very good view of what my reaction needs to be to law enforcement in my jurisdiction. And I am an American company, and I have a number of my staff in Europe, so I consider both to be my jurisdictions. I know the terrain. The case of Poland would be in my jurisdiction, even if I don't have any activities in Poland, but European police has organized itself in a way that I have to respond to it. There, I don't have a huge amount of choice. At best, I can reduce the amount of data. I can ask them for further information. When I get a police request that says, "Give me everything you have," my first question is, "No, that's too much. What do you want exactly?" But I have to answer. That's the story. And you're talking about potential political persecution, which is bad enough. It could be as simple as a cop looking for his ex-wife's new boyfriend's information to go and knock him out. It happens. And it happens, by the way, at least in Europe, a whole lot more than political cases.

MACIEJ PIASECKI: Just to add quickly, we have confirmed cases of NSO software's Pegasus being used in the way you described against legitimate political opposition, the biggest democratic party.

SEBASTIEN DUCOS: And there is no way for me to know it, except that there is a difference between a subpoena and a court order. There's a difference for me also in the way I treat it. A simple subpoena, I'm not going to give somebody's home address just like that, even in

my jurisdiction. The rest, and maybe that's my personal choice, the rest is at best like, "No, thank you." I don't see that, and I see that from most registrars. So we need to also maybe step down a bit that fantasy of the registrar that is trigger-happy and distributing registrant data left, right, and center. We don't, because these are our clients. If we were behaving like that, they would all flee. And the good and the bad, we're not just protecting people, but it's our clients. We're not giving information just like that. We would be, in our own jurisdictions, in foul of the law to start distributing information of our clients left, right, and center outside of it. We're not allowed to do it, and we wouldn't want to do it. And again, these are people we know. They're our clients. So of course, we need to be very clear and explain to registrars what they're looking at, but we can't completely forget that they're also professional people that know some of what they're doing. And it's good to repeat it, but let's not assume we're all going to distribute our data all around. Thanks.

FARZANEH BADII Thank you. I see Tapani's hand is up, and then, yeah. Go ahead, Tapani.

TAPANI TARVAINEN Thank you. Tapani, for the record. I actually have a question I don't know the answer to about the scope of data. In particular, does the GDPR distinction about special categories of data apply here, and how? Sometimes just knowing the registrant's name associated to

a certain domain name might reveal their sexual orientation or political views or something, and sometimes not. So I'm wondering how a registrar would treat that. And I'm not sure it even matters, but if it does, should there be a rule there, and how should we interpret that? And, well, okay. Question, if somebody has, like maybe Sebastien has an answer.

SEBASTIEN DUCOS

So again, I'm skipping the queue, but I hope it's all right. I have a very limited amount of actual requests. I have nine over the last six months, so that's the sliver of visibility that I have. Those requests tend to be very wide, but the wider they get, statistically, the further they are from my jurisdiction, the less chance they have of getting anything. Those in my jurisdiction, and I don't know if it's because law enforcement are better trained, they explain better what they need, tend to be quite precise. It's not everything you have; it is, "I need an email address, I need a phone number." And they're more interested in that than they are in a home address or the name of a person. I suspect because they've been trained and understand that the higher they go into the depth of the PI, the more they need to show in order to be able to get access to it. And frankly, if somebody says, "I want the home address of such and such," I won't do it with a subpoena. I will ask the cop to come back with a court order. And police were explaining here in these instances that very often, when they need to act fast, they'll pass on the information and get the paperwork after. I can't do that. I can't take that risk. So I ask them to give me more information

behind it. I suppose that once you've got a cop and a judge behind him giving him an actual court order, we've got enough rational heads to avoid the, "I'm looking for my ex-wife's new house," or something like that. But again, I can't guarantee that. And a court order is binding. I can't run away from it.

FARZANEH BADII I see. I'm sorry, Suncica, I think.

SUNCICA ROSIC Yeah.

FARZANEH BADII Oh, great.

SUNCICA ROSIC Yeah.

FARZANEH BADII Go ahead, and correct me if I'm wrong.

SUNCICA ROSIC For the record, yeah. ICANN85 fellow and also a volunteer for Project Jake. So that's a project run by Dr. Steve Crocker. And I wanted to touch upon some of the points that have been raised, specifically the scope of the data that has been mentioned. So within Project Jake, we have a requester side and a data holder

side, which is usually either the registrar or the registries. And then the data is sectioned into different sensitivity levels, where sensitivity level would mean, okay, how confidential this data is. And the way that the whole software works is that you would have a requester being part of the requester group, and then the requester group would submit a request for the data conditional on the group they're part of and conditional on the agreement that they have with the data holder. And what I'm hearing in this conversation so far is that there is an attempt to protect the registrant, but also there are cases where the registrant must disclose certain data, and therefore, there is a big burden on the registrant side, but also, sorry, big burden on the registrar side, but also an attempt to protect the registrant's data. And I wanted to ask you from your perspective, and from the feasibility point of view, how does this sound to you? Because hearing your voices and your opinion would help us think in which direction we want to implement the project further.

FARZANEH BADII Thank you. So from the NCSG, actually, we are going to go through, we are having a great conversation with Steve about this as well, and the SRT. And there are certain aspects of authentication that we agree with him, but also from the outside, we have to talk among us. But authentication of these designated user groups, it sounds like a good approach, but it all depends on the safeguards that we have and how authentication works, and also the safeguards that we have in authorization. But I think your question,

of course, we are going to go through all the stuff that we want to see in the authentication and authorization, but I think maybe Sebastien, do you want to? No? Okay. So we will discuss this further with you, and I hope we address some of your questions through the presentation. So, Stephanie?

STEPHANIE PERRIN Yes. Stephanie Perrin, for the record. I'll try to be brief. I think that way back in the mists of time, during the Experts Working Group on WHOIS that started up in 2013 and went till about 2014, we were going to Singapore back in those days, might've been 2015. And I noted with concern at the time that we had just had conversations with Interpol as to whether or not they were willing to certify, authenticate, provide some sort of cryptographic evidence or tokens that people asking for data in their name were indeed asking and had a legitimate investigation. And they declined, and the whole problem of authentication of law enforcement was just ditched during that debate. Members of the EWG might quarrel with me over my characterization of that, but I was the privacy expert on that group. So I was also very concerned that there we were in Singapore. Singapore had just been awarded an Interpol hub, and lo and behold, even today, according to Wikipedia, Singapore has still not signed on to the Covenant on Civil and Political Rights that Farzi referred to in the human rights impact assessment. So there is every reason to be deeply concerned about law enforcement being willing to make the effort to put in the authentication requirements necessary, to admit their problems

with internal fraud and internal abuse of the systems, and to guard against transfer of data to jurisdictions where there are no controls whatsoever in terms of the use of the data. And that ought to be everybody's concern nowadays. We're not talking about transborder data flow yet, but the registrars, and I'm sure they're mindful of this because they're liable for misuse of the data, and if it goes to a jurisdiction that can't be trusted, and I won't insult any countries present here by naming that list of countries that can't be trusted nowadays with personal data, particularly when we're talking about human rights advocates, it's a long list. Thank you.

FARZANEH BADII

Thank you, Stephanie. So that was a very illuminating comment, that we have to also think about transborder data transfer. And so let's go to the, what's this human rights framework that we are talking about? So we have these three elements of values of legitimacy, necessity, and proportionality. And underneath those, you will see that we can talk about, for example, the action should pursue a legitimate aim recognized under international human rights law, specified in the law, and serving a genuine public interest. And why do we have legitimacy and legality underneath it? Because sometimes it can be legal in one jurisdiction, but it might be a human rights-violating law. So what we are doing about authentication, we need to ask these things. In authentication or in the authorization, is the request grounded in a specific statute, legitimate aim under the ICCPR and ECHR and UDHR, and is the requesting authority legally empowered to demand this data? And

could this suppress political speech or dissent? So when it comes to necessity, the action should be absolutely necessary. Has law enforcement looked at other data and seen if they can do their function by using other data? And would a narrower request achieve the same goal? And then we come to proportionality. Is the scope of data limited to minimum necessary? Does it target a journalist, activist, dissident, or minority? And could disclosure map association or expression beyond stated purpose? So these are the elements that we have to consider in both authentication and authorization. And some of them belong to authorization, some of them belong to authentication when we are doing the human rights impact assessment.

And transparency and accountability are the two other elements. Should we notify the registrant if we disclose the data, if there is no court-ordered gag? Will this request appear in some sort of transparency reporting? And is an audit trail maintained for accountability? So these are the transparency and accountability stuff that we think should be considered when we are talking about authorization and authentication and the process. And I want to mention something underneath all this. You see these two lines that come from ICANN's Framework of Interpretation of human rights. Andrew, this is going to make you very happy. No core value takes automatic priority. Balancing must be case by case on the basis of proportionality without automatically favoring any single value. The result must not cause ICANN or contracted parties to

violate any commitment as said in the bylaws. Go ahead, Chris, you have a. Oh, sorry. It was Sebastien first, and then Chris.

SEBASTIEN DUCOS

So, Sebastien Ducos again. A point on having to inform the registrant or not. GDPR, for Europe at least, is actually very clear. You have to inform the registrant. There's nothing about immediacy or anything like that. Because of that, most of the requests that we get from law enforcement specify in the request that we shouldn't. It should be held. And in the US, it happens differently, but again, most of those orders are requesting that we shouldn't divulge the fact that an investigation is ongoing. Yeah, sorry. It's a bit late, and my head is not working that way. I wanted to say also to your question, Tapani, before. Even before we get requests for data, I'm looking again at all of the nine requests that I have. In those jurisdictions that are more aware of privacy protection and so on, rather than a request for data, what we have is a request to, and I had the term, I've just lost it. But basically, a request to lock the data in the sense that it can't be changed. Nobody's asking us for the data. It's a preservation request. So they don't ask for us to give the data. They ask for it to be preserved, and then they might come with further paperwork in order to get that. But that's really the first level, and the one that we see the most.

CHRIS BUCKRIDGE

Thanks, Farzi. Chris Buckridge. ICANN Board member, but just speaking from personal interest and trying to understand here. The

point I had a question about is number two there, necessity. So is the implication that registrars receiving these requests should be able to determine whether alternative methods have been exhausted by the law enforcement agency making that request? In terms of, would a narrower request achieve the same goal? I'm guessing the specific goal of law enforcement is not necessarily made transparent to the registrar, but I'm curious to understand how that works.

FARZANEH BADII

Yeah. So that would be nice, but it might not be possible. So perhaps we need to find ways to see whether in the law enforcement, and we can do that by looking at what the requests are for, what is the purpose of the request. But we can't ask the registrars to make that decision. But these are just something that they can consider when they are evaluating the request. But one thing that is funny enough, for example, if there is an alternative method, sometimes the data that the law enforcement asks for is public. So the registrar can say, "This is public information." But this is something that we can discuss and see how we want to go about it. Maybe we can do it at the authentication level. When we have a form for authenticating the law enforcement, we can say, "There should be no other alternative to access this data, no other venue." So we can do that. But these are all wishful thinking and great ideas. But yeah, you are right. That's why it's so important

that authentication and authorization are two separate processes. Maciej, is that better?

MACIEJ PIASECKI

Maciej Piasecki, EURALO again. If I understood the discussion at the SSAD working group correctly, the maximum information provided would be actual justification and all, let's say, the metadata that the police was using. But the least that should be done in terms of user interest is to notify the innocent user, not a criminal, that there was such a request issued at this date, in this case, that is now closed. Because if there's an ongoing investigation, notifying would risk that the secrecy of the investigation is violated first, and of course, if it's an actual criminal, it would provide information to them that they can use to evade justice, and that is not, of course, in the interest of users. So I was wondering what kind of notification timeline you were requesting, and I think the court order GAC provision is a little bit too thin here, because the secrecy of the investigation should be taken into account as well to help catch criminals.

FARZANEH BADII

I think, Andrew, your hand was up.

ANDREW CAMPLING

Yeah. Andrew Campling, for the record. Just reflecting on, I think, Sebastien's earlier comment that, for obvious reasons, the nature of the investigation isn't disclosed. And I'm looking at columns two,

and in particular three, and wondering how on earth you can come to any meaningful conclusions. So, for example, I'll randomly pick up one item, but just to illustrate the point. Just because it's a journalist that's a registrant, it's not inconceivable that they may also be somewhat involved in CSAM, to pick obviously an extreme example. And if the registrant isn't aware of the nature of the investigation, which they won't be, they'd have no way of knowing whether it would be proportionate to disclose that information. So absent that information, I don't see how the registrar is in any position to do a meaningful assessment.

ANDREA GLANDON No, there's no more hands up.

FARZANEH BADII Okay. So these are not going to be prescriptive fundamental rights impact assessments or human rights impact assessments for the registrars. We are just going to say maybe these are the questions you can ask. But the human rights community has worked on these questions, and there are guidelines on how to actually find that out. For example, is the registrant in a country where currently there is some political uprising? And does the country have the death penalty for political activities and stuff like that? So this is more of assessing the risk, and it's not like you can totally tell, but you can see if the risk is high or low. So we will provide some guidelines for the registrars to think through and go over a checklist. For example, if there's the death penalty or torture and stuff like that, they just

have to consider that one data point. But it has to be holistic, the human rights impact assessment. They can't just say, "No, there's torture, so we are not going to do it." If it's torture, but the guy is doing phishing, that's not going to lead to their death if they disclose the information. But sometimes law enforcement agencies, and this is what we have been saying, law enforcement agencies pretend that they want to investigate some kind of phishing, and then they get access to data. And that's why, in our opinion, authentication is very important. At least we need to tell the registrar what sort of activities that law enforcement agency does. What's the nature of the activity? Does it work in agriculture, or does it work in a CSIRT, or do they work in, I don't know if it's, oh, I was just going to mention it. Okay. Yeah. No. Let's go to the next slide.

ANDREA GLANDON Sebastien has his hand up.

FARZANEH BADII Sebastien, go ahead.

SEBASTIEN DUCOS Yeah. And again, in the case of law enforcement, I think you both made the point, these slides go way too far. There's no way. But we have to assess also requests from IP lawyers, from all sorts, and then it becomes absolutely relevant. So I don't think the slide should go, but indeed, in the case of law enforcement, they don't

invite us to the crime room. I don't get to see the wall with all the thread. That doesn't exist. I have no idea.

FARZANEH BADII Sorry, what? The slide should go?

SEBASTIEN DUCOS No. In the case of law enforcement, I have no visibility. I can't do the balancing test in a way that is significant, the way you're describing in column two and three. I don't have that visibility.

FARZANEH BADII Okay. So can I tell you something? So what if, in authentication, we try and give you that kind of visibility?

SEBASTIEN DUCOS Okay. So in that, and that is part of the discussion that we had, maybe not directly on the mic in the SSAD, but in the hallways. My personal understanding, having followed that work for the last, I can't remember how many months, but since the beginning, you were on the same calls, is that they were stepping this project into something more complicated. Right now, it was only recognizing email address, and of course, we've said that that wasn't enough. And then afterwards, it would be full authentication with levels of that authentication, that capacity to say not only what jurisdiction, but what rights that law enforcement had on data or not, and etc. That is not going to be the case. I got absolutely clear confirmation

from law enforcement this week that that will not be the case. That is way too complicated, that they're going to work on a, yes, it is a cop or no. Which is, again, and I've said it to them and I've said it on the mic, clearly not enough for me to change the current decision process that I have, because actually, I know how to recognize a cop in my jurisdiction. I don't need to be told that. Outside of my jurisdiction, super interesting, it should be a cop, but it's outside of my jurisdiction.

MACIEJ PIASECKI

Maciej Piasecki, quickly. There was a very interesting discussion at the ccNSO session yesterday where the ccTLDs, the TLD operators, were explaining how closely and successfully they work with the police, but they happened to all represent, sorry, countries that have very high standards of scrutiny over law enforcement. And those were Sweden, Norway, Canada, and Australia, I think. And the discussion was generally very happy, but I felt obliged to challenge it, as these same standards cannot be applied to the majority of the countries in the world. But what the representative of, I think, the Norwegian ccTLD told me was that they wouldn't be disclosing any information to law enforcement agencies outside of Norway.

FARZANEH BADII

And that is the problem. It's not the problem. This is where our concern is because we are coming up with a system that is global. Of course, we are not coming up with a system that automatically

discloses the data, or ICANN is in any way involved with disclosing the data. But we are coming up with a global authentication mechanism. And, yeah. So our concern is that, yes, there are registrars, registries, in countries that are democratic, and they have values, and they follow those, and they have data protection laws. But what if, when the system facilitates a global actor kind of ecosystem, then that's not going to be the case for everybody, as you said. So yeah. Hard stuff. Right.

ANDREA GLANDON Sebastien's hand is up.

FARZANEH BADII Is it up?

ANDREA GLANDON Sebastien's hand.

FARZANEH BADII Sebastien.

SEBASTIEN DUCOS Yeah. So your point is exactly that, and the same thing goes to law enforcement. We're getting taught how to behave by people who say, "But it's easy. If the cop asks, I give him the data." But it's only one because a ccTLD is only looking at their own jurisdiction. They don't even consider European jurisdiction, which I do. I'm already

done. They don't. It's only in their country. And the same thing for the cops. The cops themselves wouldn't exchange that data. They would do it now at European level, but they wouldn't exchange that data with a foreign country, certainly not under 24 hours, certainly not under the 14 days that we're talking about for general requests. It just does not happen. They ask us to go through something they wouldn't be able to reproduce in their own exchange of data. An exchange of data between Europe and India, to name nobody, is at MLAT level. MLAT is diplomatic exchanges. It's a year in the process until you get denied. And they're asking us to go and react on things that are completely outside of what they do themselves.

FARZANEH BADII

Okay. So one of the gaps, some of these gaps, I don't want to go through all of them, and they're a little bit cryptic, so don't read into this slide too much. But what can we do and how can we address these concerns? We have been discussing whether we should have fundamental rights balancing or a human rights impact assessment mandatory, tell the registrars and registries that you have to do this, but not be prescriptive. Say that, "These are the guidelines, and you should do fundamental rights balancing and human rights impact assessments." Because I think that in the RDP, in the registration data policy, there is some kind of language, and Sebastien, help me here. Is there some kind of language for fundamental rights balancing, but it's according to applicable law, right? Yeah. I think it limits the fundamental rights balancing to the applicable law. So European countries have to do the fundamental

rights balancing because of GDPR, European registrars and registries inside of Europe. The problem is that we are planning to provide this global system, but we are not providing the protection for the registrant globally. So what should happen here? The suggestion was that we get rid of "according to applicable law" and just say that they should do human rights impact assessments or fundamental rights balancing.

Another thing is creating an authentication mechanism. But what should that authentication mechanism look like? How should it look? And the conversations that we've been having, this authentication mechanism, as it was mentioned, they don't want to go beyond just verifying whether this is the law enforcement that it is claiming to be or not. But they say that that's because there is another step, which is authorization. So authentication doesn't mean automatic disclosure of the registrant data. At the authorization level, then the registrar looks at the response, the disclosure request and stuff like that, and tries to decide. All we want to do, through the authentication and authorization, is to help the registrar or the registry to decide whether they should disclose this data. And so we can also work on the submission form for the disclosure request. The authorization at the moment is in RDRS, and Lisa was here. I guess she got bored. Because I have looked at the form, but I'm just thinking, how can we make that form a little bit more elaborate and what sorts of elements do we want in that form for law enforcement in order to provide information for the registrar? For example, in that form, we could

ask the law enforcement to commit to not violating human rights with their request, and elements like that. It can be more serious. But we need to go through the form, and we need to see what sort of elements we want there. Because for the authentication, unfortunately, I don't know if we are going to win that battle. We will fight it, but whatever we don't get in the authentication, we have to see how we can bring it to the authorization. The problem with having authentication as just wanting to verify the identity of the law enforcement, the problem is that then you have this pool of authenticated, and in some people's minds, legitimate authorities from around the world that use the system. And I personally don't agree with that. I think it's a dangerous idea. I think that we should not allow law enforcement agencies from countries that are well known for human rights violations to be included, but that's a very controversial opinion, apparently. All right. Let's go to the next.

ANDREA GLANDON Andrew's hand is up.

FARZANEH BADII Is there another one?

ANDREA GLANDON Andrew?

FARZANEH BADII Andrew.

ANDREW CAMPLING Yeah. Andrew Campling, speaking for the record. The challenge is in those jurisdictions where there maybe aren't such high standards for, sorry.

FARZANEH BADII I didn't hear.

SEBASTIEN DUCOS Just the camera.

FARZANEH BADII Oh. Go ahead.

ANDREW CAMPLING Okay. Yeah. I don't think this serves a useful purpose in those jurisdictions where perhaps there are, let's politely say, lower standards, because they can just write laws to require registrars in those jurisdictions to comply. So it doesn't help there. So then you say, "Well, where will it apply?" So yes, it will apply in other places. That's lovely. But as we've sort of, I think, discussed, the human rights impact assessment, if it's involving law enforcement agencies, only really can go as far as accreditation. But any authorization is going to be in the form of a court order, I would've thought. You're not going to get much more than that. The only

place where I think it can serve a useful purpose is for non-law enforcement examples. I think the one Sebastien gave was for copyright infringement. Yeah, fine for that. But for those cases involving law enforcement agencies, I think this is going to be of very limited applicability. And in those jurisdictions where there aren't high standards, it's irrelevant, unfortunately.

FARZANEH BADII Thank you.

ANDREA GLANDON Stephanie's hand is up.

FARZANEH BADII Oh, I see. I swear she just raised her hand. Stephanie, go ahead.

STEPHANIE PERRIN Stephanie Perrin, for the record. I just want to point out that, as I said rather passionately earlier, it's a long list of countries that can't be trusted nowadays, even if they've signed on to various treaties. We have extradition treaties where our hands are tied, and we have administrations that are not respecting their international covenants. So all of this forces one to be extremely cautious about transferring the data. Thank you. I also wanted to add that some of these international organizations, like certainly Eurojust in Europe, has a privacy office that does a pretty thorough job of at least trying to police this. Europol has the same. It'd be worthwhile having a

conversation with them, but I'm sure you're going to find out that this isn't going to solve the problem, because they won't allow the level of data that the contracted parties need to make a determination, and it all leads you back to a judicial warrant and the MLAT process.

ANDREA GLANDON

Maciej's hand is up.

MACIEJ PIASECKI

Maciej Piasecki with EURALO. You've mentioned copyright infringement. It should be looked into whether sometimes it wouldn't fall also under the scope of what we're discussing here, because in Polish law, in our criminal code, we have defamation, for example. So if the copyright infringement would include alleged copyright infringement, and it would include some alleged accusations, let's say, saying that a big brand of sweet drinks is complicit with a genocide somewhere in the world, that could be classified as defamation and prosecuted as a criminal case. So these kinds of borderline cases might actually fall under the scope of what we're talking about.

FARZANEH BADII

Okay. Nobody else is in the queue. Let's go to the next slide. Okay. So let's go to the next slide. Okay. So I think I covered this one as well. Let's go to the next. I'm sorry. All right. Yay. Those are the slides I think Lisa cared about. So, okay. Imagine this is the

authentication form that I thought maybe we can discuss, and some of this stuff might have to go to the authorization process. So one is officer identity, like legal name, badge, rank, department, official government domain name, direct callback, and phone number. And then we would like to see legislative mandate. Are they authorized to access private data? Does the mandate cover domain name registration data, or in general, sensitive private data? That's what we mean by that. Is judicial oversight required for this agency, or is it administrative only? And then, of course, we can look at cross-border mechanism. And then also agency identity. What's the agency's name, agency type, criminal justice, admin, regulator? These are really important because it gives the registrar some kind of information on what is in the mandate of this agency, and I think that's really important for their fundamental rights balancing.

And another thing is that I think, since the registrars and registries in Europe do the fundamental rights balancing already because according to GDPR they have to, we need to bring them to the conversation and ask them how they do it. But I have published a report recently on this, and I have talked to a few, and it's just simple. Is there death penalty in that country? They don't disclose the data if there's death penalty in that state or country, and a few other things. And then, okay, for this authentication, then verification, anti-spoofing, these are the stuff that usually we can learn from different authentication portals like LERS or Kodex. We also suggested to maybe invite them or maybe try to learn if there's

a standardization group somewhere that standardizes this kind of authentication process, so that we can have a chat with them. Also in SSAC yesterday, we were talking about it. Anybody wants to make comments on this authentication? Yes? No? Oh, go ahead.

SEBASTIEN DUCOS So this is Sebastien again. So, first of all, watch the size of request forms, particularly if the answer is going to be no. That's always the safest way.

FARZANEH BADII It takes time.

SEBASTIEN DUCOS Sorry. No, no, no. It takes time, but what I mean is we need to also balance. If we make things too complicated, they'll find other ways. Most of the requests that I, not plugged into any ICANN system for that, but most of the requests that I get, I don't even get through the standard approach that I've dictated for it. I get an email, an info@ or something of that thrown. So the more complicated we make the system, the more chances we have of it not being used, and it goes counter. So again, everything in the first column, I believe, is already asked by the RDRS system. Everything that is beyond that, it'd be great, but I don't believe I will see it. And again, by the time I've got an MLAT, I have the equivalent of an own-at-home, my-jurisdiction type paper. It's great, but it might be overcomplicating the case because.

FARZANEH BADII But this is just authentication, so you are not doing anything. They are.

SEBASTIEN DUCOS They have clearly said that they wouldn't.

FARZANEH BADII So, yeah?

SEBASTIEN DUCOS Yeah. Yeah. That is way too far. They don't know how to do that.

FARZANEH BADII Go to the next slide then.

ANDREA GLANDON Stephanie's hand is up.

FARZANEH BADII Stephanie, go ahead. Sorry.

STEPHANIE PERRIN Stephanie Perrin, for the record. Forgive me if I'm having a bit of a Groundhog Day here. When we did the EWG back in 2013, I brought, because I had recently been an access and privacy coordinator in a federal government department, and they don't get it within

government unless they provide this, and there is a lot of quibbling over whether they have the legislative mandate. That's a problem if they don't want to admit that they are, for instance, busting somebody under child trafficking laws. But sometimes, we argued about that back then. Here we are years later, life is much more complicated. We're dealing with AI-empowered cybercrime and spoofing, and legislative body, or rather, LEA-empowered spoofing, and they won't let you interrogate them? That's not good enough. It's too hard for them? Tough shit. How can they be trusted to investigate complex cross-border crime if they can't manage a very simple form like this? Thank you.

FARZANEH BADII Thank you, Stephanie.

STEPHANIE PERRIN Excuse the language.

FARZANEH BADII No, it was great. I want to say all that. Okay. So we are going to see how we can get some of this authentication. So I'm sure they are okay with security, making sure that they have secure systems and so on. Or will they dispute that as well? So, okay. Well, I invited law enforcement, but they have another meeting. I will send the recording, and we can have more conversations about this. But whatever we don't get in the authentication, we can see how we can ensure that we have more data elements in the authorization.

Because the authorization process is the process where the registrar decides whether to disclose or not. Sorry, I sound like a broken record, but I keep having to mention this.

So now, what should this system, the request form, have? So legal instrument, if they have a subpoena that is just for the subscriber info only, court order, search warrants. Generally, search warrants, and this is based on US law. But I think that for GDPR, I should not have done this based on a single jurisdiction. I'm sorry about that. So they should do fundamental rights balancing for all of these. Do you know, Sebastien, if the form allows you to upload legal instruments like subpoena and court order? It does?

SEBASTIEN DUCOS Yes, it does. Yeah.

FARZANEH BADII Okay. So.

SEBASTIEN DUCOS Yeah. No, yes, it does. No, sorry. The current form doesn't because of ICANN liability. The RDRS was built outside of policy, and anything that could have PII is not, yeah. Sorry. I would have to check, and again, it's late, but I think that for legal reasons, ICANN preferred not to do it. But this doesn't mean to say that it wouldn't in the future, because in the SSAD, it was planned to have it. ICANN

is only willing to do it under policy. Long, long answer. It's not today, but it should be.

FARZANEH BADII

Okay. So the data scoping. So this data scoping is kind of redundant, because I think the RDRS just allows for the data elements that are just in the policy, right? So the data scoping, would that create any problem? No, I don't think so. And then the necessity statement. We wanted a necessity statement. So you remember that I said that it should be necessary. So it would be good for the law enforcement to answer what alternatives they tried, why infrastructure data is needed, why at this layer they need it, and by this layer, I mean this geeky thing that we say, meaning at this technical layer of the registries and registrars. And then the purpose limitation. They should state the purpose, and they should commit themselves not to use it for secondary use. No onward transfer. Actually, that was your point, Stephanie. No onward transfer, and retention deletion commitment. They should delete it after a certain time.

And yeah, of course, this is a draft, and we can discuss it with NCSG and then go and talk to SRT. But these are the elements that we think could be good to have in the form. So some kind of commitment to purpose limitation and stuff. And then the human rights impact assessment that I was talking about. Then the registrar can decide, okay, so what's the jurisdiction risk? What's the registrant profile? Is it a journalist? Is it an activist? Is it a

dissident? I can't see the last one. And then is it necessary? Were there alternative investigative methods exhausted? And they can decide that based on the answer that they get in the authorization form. Okay. And I don't think there is a next slide. No. Okay. Right. I didn't go over our transparency request, but we want the RDRS or whatever system comes next that replaces RDRS to have, they do issue these reports, I think it's on a quarterly basis. And we want more transparency on data elements in that report. What's the purpose of the request? What are you going to use it for? Is it a hate crime or is it cybercrime? And also, when the law enforcement gets their authentication and stuff, if we cannot have elaborate authentication, then we want some sort of transparency, like what sort of law enforcement agencies from what countries. It can be at aggregate level. Submit these requests so that we can see how risky the system is. Yeah, Andrew, and you have two minutes because we have three minutes to finish. Go ahead.

ANDREW CAMPLING

Okay. Sorry, real quick. Unless I'm missing something, I think in the authentication step, from what I'm hearing, probably a hypothetical registrar might determine, as soon as they realize the request is from a law enforcement agency in country X, the answer is no, so they won't do this. And similarly on this page, I presume, and maybe we could comment on this, if there's a court order, then the rest of this is also irrelevant.

FARZANEH BADII Yes.

ANDREW CAMPLING Because.

FARZANEH BADII Absolutely.

ANDREW CAMPLING There's a court order.

FARZANEH BADII Yep.

ANDREW CAMPLING So the judge has presumably done something like that.

FARZANEH BADII Yeah.

ANDREW CAMPLING Anyway. So this only really is applicable if you think that the requesting jurisdiction is, by your personal definition, acceptable.

FARZANEH BADII Mm-hmm.

ANDREW CAMPLING And if it's not supported by a court order. And even then, as we discussed earlier, if it's a criminal investigation, you won't have mostly the information to do a meaningful impact assessment anyway. So I think, in other words, I'm just saying this is fine, but I think it's going to be applicable in a very narrow subset of cases.

FARZANEH BADII Yeah, absolutely. And many of these things that we are saying, they are very narrow. Go ahead, Chris.

CHRIS BUCKRIDGE Chris Buckridge. And just even in those narrow cases, it's essentially a best practice?

FARZANEH BADII Yeah.

CHRIS BUCKRIDGE Yeah.

FARZANEH BADII Yeah.

CHRIS BUCKRIDGE Okay, so there's no enforcement, there's no requirement. This is simply for registrars and law enforcement that, okay, cool. Thank you.

FARZANEH BADII We are not going to be prescriptive, and we've been saying this. I think some others want to be prescriptive. The other day, we were surprised. We would like to see some kind of enforcement, but we don't think it's possible now. So we want it through transparency reporting and telling the registrars how to do the fundamental rights balancing and stuff like that so that they do it. But they have to do the fundamental rights balancing. It is there. They have to do it, and we want it to be global, but we are not going to be prescriptive on how they should do it. Yeah.

CHRIS BUCKRIDGE Just trying to understand.

FARZANEH BADII You want to take that as well away from me, or?

CHRIS BUCKRIDGE But I am just trying to understand, when you say they have to, in what sense is the compliance enforced?

FARZANEH BADII Yeah. It's aspirational.

CHRIS BUCKRIDGE Okay.

FARZANEH BADII But we want to check it with transparency reporting and stuff like that. We want to have some kind of mechanism in place that is a soft mechanism that we can see what is the state at the aggregate level, all the registrars. Are there many law enforcement agencies that are human rights violators that get access at the aggregate level? We are not asking very much. All right. I think we are done. I think this session actually was very useful. I found it very useful. Oh, yeah, Maciej, go ahead.

MACIEJ PIASECKI The session was very useful indeed, but we are in the most remote room of the venue at the end of the meeting, and with the title, which is even less appealing than the review of reviews. And I think this is very important for the end users and should be especially interesting to some of the fellows, so I suggest that it's going to be promoted further. Thank you.

FARZANEH BADII Yeah. We had a great conversation, and thank you so much for all your questions, and thanks for attending. Oh, Rafik, go ahead.

RAFIK DAMMAK Yeah, thanks. Thanks for presenting, thanks for everyone for making it, but just to respond quickly. We don't control the room, and we just make a meeting request, and we had to make changes because of a lot of conflict. So that's the limits and constraints we have to deal with. Saying that, I guess for the next ICANN meeting, we'll try to have the town hall.

FARZANEH BADII Yeah.

RAFIK DAMMAK And we'll plan ahead. So to see, maybe early in the week. And yeah. We'll try to prepare and have more attendance, hopefully. And yeah. With that, thanks everyone. And now you are free, and enjoy the rest of your day.

[END OF TRANSCRIPTION]