
ICANN83 | PF – GNSO-Human Rights Impact Assess-Navigating Disclosure of DN Registrant Data
Thursday, June 12, 2025 – 15:30 to 17:00 CEST

ANDREA GLANDON

Hello and welcome to the Human Rights Impact Assessment: Navigating Disclosure of Domain Name Registrant Data Session. My name is Andrea and I am the Participation Manager for this session. Please note that this session is being recorded and is governed by the ICANN Expected Standards of Behavior and the ICANN Community Anti-Harassment Policy.

If you would like to speak during this session, please raise your hand in Zoom. When called upon, virtual participants will be given permission to unmute in Zoom. On-site participants will use a physical microphone to speak. Please state your name for the record and speak at a reasonable pace. And I will now hand the floor over to Farzaneh. You may begin.

FARZANEH BADIEI

Thank you very much, Andrea. Hello, everybody, and welcome to the Non-Commercial Stakeholder Group session on Disclosing Private Personal Domain Name Register and Data to Third Parties and Human Rights Impact Assessments. This session was as a result of many conversations and discussions that we have had throughout ICANN meetings and with other stakeholders about how can we disclose the data in a rights respecting manner and

Note: The following is the output resulting from transcribing an audio file into a word/text document. Although the transcription is largely accurate, in some cases may be incomplete or inaccurate due to inaudible passages and grammatical corrections. It is posted as an aid to the original audio file, but should not be treated as an authoritative record.

what the registries and registrars are doing about that and what are what can be the best practices, and also like what are the current frameworks that we have that registries and registrars can use. And what is the path forward?

It's a conversation starting session, I don't know if that's correct, but we are just going to start the conversation and we are going to have many more sessions and dialogue about this. But we thought that it would be great to have all experts in the room, to have your opinions and practices that you follow in order to disclose their private personal information of domain name registrants to third parties. So the session, we might divide it into two segments, it depends on how we want to go about it and how you feel energetic to go into breakout groups or not. So in the first segment, we are going to have a law enforcement perspective. They are going to announce from the Greek cop, what is it? Hellenic police.

And I have to thank the Public Safety Working Group for cooperating with us. And all the time, whenever we invite them to these sessions, they are responsive and they want to engage. And you don't see that in many places, so thank you so much. And so we are going to have Nome to talk to us about the challenges that they have, also the process through which they request data. And then we are going to have a registrar perspective, how they do a balancing of rights in disclosure decision by Reg Levy from Tucows. And then a registry perspective on balancing rights in disclosure

decisions by Kristian. Was that good? Great. From .se, of course. And Michaela is an NCSG member, but also works with Article 19.

And Article 19 has come up throughout the years, has come up with different frameworks for Human Rights Impact Assessment for disclosing data especially in the registries and registrar setting, and Michaela can go through those frameworks. We want this session to be also useful for other registries and registrars that are dealing with these issues and disclosing data to use these best practices, and hopefully we can come up with some guidelines on that that registries and registrar can use. And then the interactive segments, we have some scenarios that we are going to give you a role and you don't have to participate in the breakout groups. If we see that the room has the energy to do it, we will. If we are having a good conversation, we continue having the conversation.

But the scenarios are really good. Michaela has come up with them. When we do the scenarios, then it kind of makes it more tangible for people to understand what is at stake, because sometimes when we talk about human rights, people are like, oh, well, we don't do child labor. But this is not a matter of that, it's about freedom of speech, it's about privacy, and a range of human rights issues.

Oh, and to our remote participants, if we go to the breakout sessions, we will also involve you and send you the scenarios to work on, but you need to have somebody who can brief us. Okay, without further ado, let's go to Noam from Hellenic Police to tell

us a little bit about the processes and also the challenges of requesting data.

NAOUM MENGLOUDIS

Thank you for the floor. I'm Noaum from the Hellenic Police, the cybercrime unit, and I'm a member of the PSWG. I represent the European Law Enforcement Community on child sexual abuse specifically, this is my domain. Can we go to the next slide? According to our local law in Greece, we have a very specific code of conduct and a very specific process dictated by law on how we do our investigations and who we can order us to take out action and when and how we take action.

Specifically for domain name disclosure requests, when we need to make a request, we always ask for the registration information from the register officially on our official agencies letterhead, and we also give a small description of what is the problem or what is the offense or what is happening, why we need the information. Sometimes we ask for it on our own like the police because our law says that if we see that something is going wrong and we can act, we should act immediately.

So we preserve all the evidence and information and then we inform our prosecutor who validates our decision or if it is an ongoing legal process, the prosecutor directly may give us an order that you should get this domain name registrant information because there is some legal case against it. So either way, the prosecutor is being informed of our actions. Then when we send

the request, we send it officially from our, if there is no, for example, some electronic service providers have a specific law enforcement portals. If there is not a portal, we communicate the disclosure request directly to the registrar via our official email.

Our agency, the sub-agent unit of the Hellenic Police, is the single point of contact for such requests to online service providers. For example, if a local police force needs to acquire some information, registrant data, they talk with the prosecutor and they order an agency to make the disclosed request. So, probably most of the online service providers will know about us or they can verify who we are because it's not like a random request, it's a specific request from a specific unit, from a specific email. In the case of urgent requests, as I told you earlier, police has the right to act on itself.

For example, our unit, because it's 24/7, we have a call center 24/7, many times we get phone calls or we get emails from civilians that, oh, I saw this online, I saw this on this forum, this person is stating that he or she will commit suicide, please do something about it, for example. So we have to investigate immediately, gather all the data, locate the person. Sometimes if we cannot locate him any other way, we have to get, for example, maybe the domain register information so we can contact him and maybe he has access to the log files of the site or it depends on each case. So we act urgently, immediately, but afterwards we inform the prosecutor with all the paperwork. Let's go to the last slide.

As I told you, we have always a public prosecutor supervising every case. And for accountability, every action that a police officer does leaves a trail on the system. For example, if he sends an email, you can see the email. We always print it on paper format because there's a case file in paper form that goes to the prosecutor to review all the actions. So, like if he orders us to do something, request some disclosure information, he always gets the request and the results back in paper form. So you can do a full audit if something goes wrong and this is required by our law. And we always try to give as much information as we can to both parties.

If I make a request to a registrar, sometimes if I have a prosecutor's order, I may just say that this offence is going on and very basic details about the case so they know what is going on and why we are requesting information. If there is something urgent, we usually provide more information, maybe some screenshots. or they can, like registrar can verify themselves what's going on by visiting a URL or looking at a post, for example, if there is a threat to life. Or, for example, if it's child abuse material online, anyone can just load the site, and will verify this abhorrent phenomenon.

And the count of conduct of Hellenic police, since we are talking about human rights, like the first sentence in the count of conduct of the Hellenic police officer, it says that that the protection of human rights is the most important parameter to ensure that you have a peaceful society and everybody can live well with each other.

And as a last comment, I want to say that human rights goes both ways, it's not only the human rights of the suspected offender or the perpetrator that is behind the domain name. It's also the human rights of the victims, which in my domain, which is child abuse, we can all agree that.

But these are more important because we had many cases that we were investigating cases of child abuse, we were even going to inside houses and asking the residents there if they knew something because maybe their Wi-Fi has been abused and their IP has been logged. And the prosecutor was ordering us to investigate everything, and not once have they complained that their human rights are being trespassed, because when we explain them that we are looking about this and that and things that are involved, they always say, okay, yes, do what you want, do what you can, I can help you as much as I can. So sometimes, even the subject itself may give away their human rights if there's something important behind it. This is my perspective.

FARZANEH BADIEI

Great. Thank you so much. So we are going to go to the other panelists and then we can have a conversation. So, Reg, you have received a request from Hellenic police. What's going to happen next?

REG LEVY

What's going to happen next? I love that. I wanted to first call out. I wanted to first call out an appreciation for the fact that the Code of Conduct explicitly talks about human rights, and that you spoke about the human rights of both the victim and potentially even the perpetrator, that everybody involved in this is a human. So my receipt is of foreign law enforcement. So to some extent, the way that I would treat him is exactly as I would treat a local lawyer asking for information, he doesn't have legal rights over the data that I hold.

But I'm also going to look at what the actual request is, and I think earlier he said something about a suicide, a threat of suicide. So that is an immediate action, and I'm going to look to see what it is that he's asking me to do. Is he asking for some information? Is the information about a person in Greece? Well, then maybe this is something that I'm just going to give to him, even though there's no "legal right" because from the standpoint of human rights, that would be a good thing to do, I'm trying to protect someone who's in danger. If the registrant information is in California or in Brazil, it may not be as relevant to a peace officer in Greece.

So I might have a back and forth and say, I'm not sure that this is the information that's going to be useful to you. Typically, this would happen over the phone and not via email, so I'm not going to be sending an email waiting for business hours to pass in Greece and then waiting for me to get back online and business hours in

California. But I always look at the actual context of the request as well as the information that we have on hand.

So I don't know what the answer is, I don't know if you're going to get the information because I don't know what the actual request is and I don't know what the actual situation involving both the domain, is it a new domain, is it an old domain, and the information and where the person whose data rights might be affected are.

FARZANEH BADIEI

Great, thank you. And so, what sort of cases, if you can talk about this, what sort of cases would kind of trigger fundamental rights balancing?

REG LEVY

So I honestly don't necessarily think of it as fundamental rights balancing, although maybe that is how I think about it. It's more a matter of I have information, there are rules that I need to follow, there are duties that I owe to my customers in terms of what I do with their information. And so I'm looking in each case at the situation involved, maybe its fundamentals that is a balancing of fundamental human rights.

But I think of it more in terms of what do I owe my customers? And my customers as a wholesale registrar are my resellers. And what do I owe their customers? So it might come into the equation who the reseller is because they like to take a more proactive approach or a less proactive approach, or they are in Greece. And so I can say,

actually, I have someone who has way more and better and relevant information for you, so why don't you go talk to this person?

FARZANEH BADIEI

Okay, that's very interesting. Thank you. Okay, we can go to our next speaker, Kristian.

KRISTIAN ØRMEN

Thank you. My name is Kristian Ørmen from the Swedish registry. So we have our WHOIS data on companies completely open. We try to keep it correct as possible. But if a domain name is registered by a private person, all the data is hidden. Also, the data on companies for email, phone number, and contact person is hidden because it could be personal information. We do get around 20 to 30 requests per month to disclose data on these registrations. And most of these requests is handled by my team in registry services, but a small handful of them, we do need help from our legal team to handle them.

In this case, we look at each request on a case-by-case basis. It is very rare that we get a request that is a legal obligation, but it could be, for example, pharmacy regulators or chemist regulators that do have some legal rights to ask for information in special cases. But most of the cases we get in don't have any legal rights to the information. And in these cases, we do look at if the request has a legitimate interest to obtain the data, so we can disclose it. But we

do look at the data from each contact, like for that interest or that purpose, would they need a name or only the email address, do they actually need the postal address.

So we look at each data field if we think that they have a legitimate interest in those data. It very much depends on the case, of course, quite often we refer them to use our contact form where we can forward their contact information to the registrant instead of disclosing to the registrant because that would, to start with, be a much better solution. With the police request, quite often they also don't come with a court order. They come in an investigation, for example, and even here we do ask them for the purpose, what are they going to use the data for, what paragraph is the investigation they are looking at right now.

So we look at all that data together before we decide if we want to disclose the data. We did have one time many years ago, the tax authorities in Sweden did ask for a copy of registrant information for all domains. They did try to put a legal binding note to that, but we took it to court, so we didn't have to give out the data. So in general, we do try to protect the data as much as we can. We take every disclosure request and look at it case by case. Quite often, we use several hours on discussing the more difficult cases.

For us, it's not important if it's Swedish police, Norwegian police, or so on, it's the purpose on why they need the data and if they have a clearly legitimate interest and a rightful purpose for the data. The more difficult cases is quite often journalists that are trying to

maybe find some background on different activities online, where we often also ask them if they are going to publish the data, what they are going to use it for, if they are going to contact the registrant, and so on. So we use quite a lot of time on each request.

FARZANEH BADIEI

Thank you so much. So is there a specific framework that you use? And also, I'm going to just ask this question, do you differentiate which law enforcement agencies to send you the request, like the reputable one or the authenticated one versus the unauthenticated one?

KRISTIAN ØRMEN

Well, since we do look at each case, case by case basis, and we do get requests from law enforcement from other countries, and since we do base it on legitimate interest, it's more the case than what country the law enforcement is coming from. But of course, if we feel that it would be an issue with a specific country or something, we could maybe refer them to contact Swedish police instead, so we could talk with Swedish police directly. But that very much depends on the case, how we would react.

FARZANEH BADIEI

Thank you so much. So, Michaela, I'm going to pass it on to you to tell us a little bit what sort of human rights framework the registrars

and registrars can consider in order to make a decision about the disclosure.

MICHAELA SHAPIRO

Amazing. Thank you so much, Farzan, and thank you to my co-panelists for laying this out so clearly. And one thing that stood out to me from all of you who have spoken already is this very-- this is fantastic from my view that you all take this very seriously and take it on a case-by-case basis, which I think is really important because something that comes out of these discussions is that it's so important to contextualize these kinds of requests. No requests are the same. And the kinds of questions that you're asking are exactly what we should be asking when we're considering a request that comes in for data.

Why do I say that? Well, I also wanted to take a second to maybe step back because I am also aware that we're very lucky to have some newcomers in this space who are here at this meeting. I'm not going to pick on them, but we're really excited that they're here. And I would also like to do a little poll just to get a sense of temperature check in the room, so how familiar we are with these. I won't make you get up, I'm not going to make you move very much, I promise. But what I was thinking is just raise left arm if you agree with the statement. So take it as this is a very excited yes.

And two arms, absolutely not, I'm done. Goodbye. So I'm going to just read a sentence, and if you could just humor me, I would just love to get a sense of kind of where people are on these topics in

the room. So first sentence, I am familiar with the Human Rights Impact Assessment. This is amazing. Fantastic. Thank you so much. And for those of you who raised two hands, I'm so glad you're here because I can talk you through more of it. So, I believe that requesting domain name registrant data can have potential human rights implications. So two hands is no, sorry. One hand is yes.

So Farzaneh is showing her true colors here. Thank you so much. And last one, I can name an example for which an urgent request for registrant data is needed. Sorry, I can read that slower. I can name one, an example for which an urgent request for registrant data is needed. Mmm, you know what? Take it as you will. What would you prefer? Actual. Then I can name an actual scenario. Okay, I can name a theoretical example. Sorry, I don't know where it's actually. No, sorry. Thank you. Great, thank you for humoring me. I know. I'm sorry. The caffeine clearly hasn't hit. So thank you so much.

Where I wanted to be able to gauge is I'm assuming if you're in this room, you have an interest in this topic, you have maybe a vague sense of human rights, and you're excited to talk about it and learn about it more. So thank you so much for humoring me. So what I wanted to kind of go through, as Farzaneh mentioned, is there are human rights frameworks that we can use as inspiration and as reference points when we go through these kind of balancing exercises.

But I'll say that my co-panelists, whether they're using the official terminology of Human Rights Impact Assessments, they're already doing this work by asking the questions about who is this request coming from, why are they asking for this data, the scope of the data that they're asking for, whether it's urgent and how we define that, and that's something I'd love to delve into more in this conversation. But those are all the kinds of questions that you need to go into when you do a Human Rights Impact Assessment. It's all about understanding who are the stakeholders that can be impacted.

Sorry to use the word in the definition, but whoever can be impacted by the decisions that are made, whether to comply with a request or deny a request. And so the frameworks that Farzaneh was mentioning as an example, and this work predates my time here, so I take no credit other than affiliation, but Article 19 did some work a few years ago to develop a registry/registrar human rights assessment tool. And so here they go through a number of different issue areas, including registry and registrars as procurers of goods and services, as an example, their employers.

They also have impacts on the environment as part of their work. And one area is around access to information. And so what that section talks about is thinking about, exactly as we've already been thinking, exactly as we've already discussed, is there a lawful request? Is this in compliance with international legal standards? What kind of privacy implications would disclosing this information have on the registrant? And one other element that hasn't come up

yet, but I'd love to kind of put forth to our panelists and others in the room, is one element that this tool talks about is transparency reporting about the requests that come in.

And we also understand that there's substantivities around that, but I wanted to put that suggestion out there because I would also be curious to see if this is something that registries and registrars are already tracking, or if there's a need for more tracking on that work that could either happen within or in addition to the work at ICANN. To understand, what kind of requests are coming in, what are the issues that are requiring a request for data, and why or why not have registrars and registries complied with these requests?

So, those are the kind of questions that all form part of a Human Rights Impact Assessment report. So that's one tool that we have at our disposal, and of course, anything that I mentioned here that there's documents that are publicly available, very happy to kind of circulate them, and hopefully maybe we can attach them on the page with the recording. But I will pass the phone to, hmm, the phone, the mic to Farzaneh. Sorry so I'll just keep going, but another resource that we have for this work. Oh yeah. Sorry, go ahead.

REG LEVY

Thanks. Reg Levy from Tucows. On the standpoint of transparency reports, a lot of the requests that we get come in in an informal manner, and so although some of the people in this room may be familiar with our tri-annual report on certain types of requests for

data that we publish right before each ICANN meeting, most of the things where we get subpoenas or warrants or informal requests from law enforcement are completely untracked. So we don't have a good transparency mechanism from that standpoint.

But in every case where a disclosure is made through the system that we created specifically for the disclosure of previously public WHOIS data, which we call the Tiered Access Compliance and Operations or TACO, it automatically sends a notification to the registrant. So if, as an attorney, I make a request, they will receive notification that Reg Levy from the law offices of Reg Levy has made this request, and it will have my office address in there and a phone number and email address where they can submit their request about, like, why did you want my data?

If it's foreign law enforcement, it will typically say, just the Hellenic police and no additional information because they don't need to know who you specifically are, and that could potentially put you in some sort of compromised position for them to know that. And if it's local law enforcement, they may have the option, depending on how the request is made, to just have the report that the information was disclosed say your information was disclosed.

So it won't even say it was disclosed to local law enforcement, it'll just say it was disclosed. If a completely secret request needs to happen, it needs to happen outside of that system because we very specifically built the system to automatically tell people that their data had been accessed.

NAOUM MENGOU DIS

So there is an option for a non-disclosure if it's an important case or it will ruin the investigation.

FARZANEH BADIEI

If anybody wants to comment on this. Do you want to comment on this? Okay. Anybody else? Okay. Go ahead, Michele.

MICHELE NEYLON

Yeah, thanks, Farzaneh. Michele, for the record. We haven't ever published a transparency report, but we have actually been tracking all law enforcement and consumer protection/legal requests that we received. We don't track every single abuse report that we receive, we do have it somewhere, but I wouldn't be able to produce a usable anything from that because Zendesk is a wonderful piece of SaaS software that's not designed for that. But for the other ones, we do track them, and the volume that we get is not particularly high, and the vast majority of them have nothing to do with domains.

Most of them are to do with IP addresses. So we get law enforcement requests about IP addresses, mailboxes, various things like that. Actual domain-related ones, very, very, very, very small volume, because ultimately, you're much more interested in all the other activity, the actual domain name itself, not so much.

MICHAELA SHAPIRO

Yeah. Did anyone else want to come in on either kind of commenting on a general trend or to kind of talk about if you're here from the registry registrar perspective? Yeah, please.

HISHAM IBRAHIM

Hello, Hisham Ibrahim, RIPE NCC. I heard the word IPN, got triggered. I'm new to this space, so my questions could be basic or could have been covered already, but I have two thoughts and I'd love for the panelists to expand on them. We heard that cases get looked on in a case-by-case space, and we also heard about looking into what agency is asking for that. How do you deal with cases where the country that could be asking the question could have different norms or values or laws that might put the person in jeopardy if you answer their questions?

And do you feel that you can make that distinction yourself or not? That's a general question. I'm not looking to anybody specific, I'm just asking the question. The second one is regarding e-evidence, which is coming into effect in Europe. It's a mechanism that allows for more exchange of information to help combat cybercrime. But then how does that work with the rest of the world and the balance that should be struck? Two questions that I would love to get some more feedback to learn from. Thank you.

KRISTIAN ØRMEN

This is Kristian from .se. I can try to answer the first one. So since we always ask for the purpose of the data, and then we use that to

try to determine if we can disclose the data or not, and that's also where I earlier said at some point we might refer this, for example, foreign police to contact Swedish police instead because then they can do the assessment of that foreign state before they contact us with a more lawful request. So we do get a lot of heat for saying no many times, but it is definitely better to say no one too many than saying yes one too many.

MICHAELA SHAPIRO

Did anyone else want to come in on this question? Yes, please go ahead, Reg.

REG LEVY

Yeah, so similar to Kristian, I typically will say if foreign law enforcement needs to keep something secret, they should go through the process with my local law enforcement because my local law enforcement has the ability to force me or rather to keep me from being able to disclose, but they can't just ask nicely. I mean, they could just ask nicely, but I don't have to do it at that point. And the way the due process works in the United States and in Canada is typically that they have to prove to a third party that it should remain secret.

So I understand that that is a longer process and that involves jurisdictional issues, but in the same boat as Kristian, in in the sense of I would rather give out less information than more information.

I see a hand, but I had another point, and it's gone. Go ahead. No, that's fine.

MICHAELA SHAPIRO

Sorry, did you want to come in?

NAOUM MENGOU DIS

Just about the e-evidence question, because we don't have all the specifics yet, it will be like a more versatile automated system for evidence transmission and evidence requests between countries in the EU. But probably it will still be bureaucratic and like for urgent cases, I don't know how well it will work, especially how interoperable it will be with outside foreign companies to the EU. We'll see how it goes.

MICHAELA SHAPIRO

Thank you. Did anyone else want to come in on this question? Yeah, Michele.

MICHELE NEYLON

Yeah, thanks, Michele, again, for the record. I think just first off, it's going to depend a lot on what the request is in relation to. So before I go any further, I'll just make that clear. So, like, if you come to me saying this is to do with a serious case of child abuse or life and limb, death is coming, something cataclysmic, I'm going to treat it very differently to, I'd like to know who had this IP address or domain name at this particular time over a fake Gucci bag. Like,

fake Gucci bag, way down my list of priorities, life and limb, death, these are things I might care about, just so we're clear.

Generally speaking, I think a lot of the registrars will deal with law enforcement from their local jurisdiction very differently to law enforcement from overseas. However, we all have terms of service, and in many cases, the investigation, the alleged crime will probably breach our terms of service. So if you can't get a domesticated order or something through our local law enforcement, you can go to us on a terms of service thing.

You can also come to us and ask us informally, do we have data? Because there's no point in you getting an MLAT or whatever for something we don't have. I spent two days in Dublin in the forecourts for an MLAT, for a domain name that had nothing to do with my company. It was great sport, and I really enjoyed the day out, but I don't think the Polish police or the Irish court system did. It was pointless. Whereas if they'd contacted us informally, we could have simply said, no, we don't have it.

MICHAELA SHAPIRO

Thank you, Michele. And you brought up a few points that I would love to pick up on after this. So I'm going to put it out there because I want people to remind me if I don't come back to this, about the terms of service and the jurisdictional issues/questions. But first I'll turn to, I think, yeah. Gabe, you'd like to go? Go ahead.

GABRIEL ANDREWS

Hi, this is Gabe Andrews, co-chair of the Public Safety Working Group and U.S.-based law enforcement. And I just wanted to add on to what I'm hearing from my friends in the registrar space that I think it's well-recognized and appreciated that sometimes you need the flexibility to say no if a request is coming from a country that you might feel doesn't respect human rights. And I think in their position, there's a few that I might find would be in that category, from my own opinion. I'm not going to enumerate them.

That said, when there is perhaps-- you're feeling sort of on the balance, whatever situation where you might respond to your local police, but you have a challenge of responding to anyone that's not the local police, there still can be great value in a swift no if that swift no is saying, hey, no, but if you talk to my local police, maybe this this can be actionable, or to Michele's point, no, but I don't have this information anyway, so it's not worth following. But the reason I say this is because I know my own agency, we have deployed agents in embassies in, oh gosh, what's the number, like 56 nations scattered around the world and they maintain relationships with local law enforcement.

And it is not trivial for me to call them up and get people on the phone like immediately, but if it is a threat to life or something serious, like I'm pulling every available string, and a swift no, if it's swift enough might be trivial compared to the amount of time I'm now playing the phone tag game, and it might still be successful in the end if it's fast enough. So I just figured it was worth mentioning.

MICHAELA SHAPIRO

No, absolutely. I appreciate that. And I think between both Gabe and Reg, that kind of relationship with the local law enforcement is very clearly a theme that's emerging. I wanted to just pause there in case were there hands online. Oksana, yes, please go ahead, and then I'll turn to you.

OKSANA PRYKHODKO

Yes, thank you very much, Oksana Prykhodko, European Media Platform. Digital human rights are a priority of our organization, and it was very interesting to discuss them in peaceful time. But I'm from Ukraine, and for four years, my country lives under war time. And four years ago, we can't imagine that we can discuss such scenario, but just now, I propose to you to think about it, about forced disclosure of data for unlaw enforcement of another country. 20% of my country just now is occupied, temporarily occupied, but occupied, and under such circumstances, it's extremely serious, and please think about it also. Thank you.

KRISTIAN ØRMEN

This is Kristian Ørmen from .se. I used to work in Denmark also, and just a quick explanation on how law enforcement are so different. When I worked in Denmark, we also got a request like this from law enforcement, and we had a good relationship with them, we always just said, no, but give us a court order, and they would be like, can we just email it, or do we actually have to come to your office?

And they would usually quite quickly get a court order, send it our way, and we would respond swiftly with the information they needed. So at that registrar I worked at, we were covered, that was nice. In Sweden, if you do the same thing, but then we have to come and take your service to look at it if you don't give it out voluntarily.

So the cooperation with law enforcement is very different in Sweden than when I used to work in Denmark. I was quite surprised about it, but of course, we try to work with the Swedish police as good as we can, but the relation is way different than what I was used to from my home country.

MICHAELA SHAPIRO

Yeah, go ahead.

SEBASTIEN DUCOS

Yeah, so I wanted to turn the tables a bit, and I'm not picking on you, but you're sitting here. I would have picked on Gabriel easily, but he left. So imagine the question comes to you, you're his local enforcement, say, how do I deal with this case? So how do you deal with a case from a jurisdiction that is not yours? And a question asked, exactly the type of question that Ishan was talking about with potentially harming somebody, how do you answer that? And can we learn from you on answering those questions?

NAOUM MENGOU DIS

Yes, so you are asking how we would handle a request from a foreign law enforcement, for example, to our local TLD registry or something like that. Yes, this is--

SEBASTIEN DUCOS

No, no, so you're talking about child abuse, for example. So you imagine from a country that has different standards, that has different views on what is and what is not, says, hey, I absolutely need this data, your registrar here is pushing me on to you, take the decision and tell him to give it to me.

NAOUM MENGOU DIS

Yes, we've had many of these cases, maybe not including registrars, but they can ask for any other information, like if someone is in our files, or like to check if someone leaves somewhere, or maybe give them back their subscriber information from an IP number, yes, usually, in our case, there are two main roads. For example, it's the judicial way, which maybe what they ask should go through an MLAT. But as police cooperation between two police forces, there are some bilateral agreements, which I can give them the information unofficially as intelligence.

They can use them, but they cannot present them in their legal process in front of court. If they want to do that to use it for judicial legal proceedings, they have to ask them officially, for example, via European Investigation Order or an MLAT. But most of the times we talk with, because even if we get a request, for example, if I get

a request for a subscriber behind an IP, I cannot get the subscriber information from our local company.

We have to go via prosecutor because the prosecutor has to give the order to the local company to get subscriber information. This is in the Greek law. For example, in Germany, they can just get the subscriber information from the IPs because it's like for seven days they do not keep logs. We keep them for a year, but we need a valid legal process. So if a foreign law enforcement asks me for something like that, I may have to inform the prosecutor and initiate legal process on our side, just to give them unofficially the intelligence and tell them if you need them for them to go to court, do it via MLAT. It's a bit like law, it's complicated.

And most of the time, sometimes they do not even give us the full picture, so our prosecutor asks, even if it's child abuse, most of the time we just need the abuse material, because in different jurisdictions, child abuse is considered differently. Of course, there are some standards. So maybe we have to review their evidence and tell them, no, we cannot help you, it's not illegal like in our jurisdiction. It depends, as usual.

GABRIEL ANDREWS

Yeah, I think you're hearing there's complexities involved. One thing I will note is that we've mentioned MLAT a few times, and if people aren't very familiar with that, I figured it was worth 10 seconds. There's the notion of the mutual legal assistance treaties, these are bilateral arrangements between nations that respect

each other's processes enough to say that, yes, if you go through these formal channels, we will take your request and we will action it to the best of our ability.

And it goes through extensive review through the Department of Justice of the entity that sends it and the one that receives it and so forth. Because of that extensive review, my anecdotal experience of having done a number of these over the years is 6 to 12 months for the process to go through. So this is something that is an effective mechanism at the end of an investigation, maybe to go through and get all the evidence in a proper way. It is not an effective mechanism to prevent imminent harm, but just to clarify, it's a tool available, it's just not always the perfect talk.

MICHAELA SHAPIRO

Thank you, Gabe. I saw a hand down there, and then Sebastien. Okay, perfect. So one, two, three.

ROB GOLDING

Rob Golding for the record. Thank you to the panel and particularly to the Hellenic Police for having a sensible, robust, and auditable policy that makes life so much easier in general. Do you have any gut feeling of the percentage difference between requests that are complied with that come with a prosecutor's orders versus those that don't? And also, do you have an idea of how many times disclosure has helped a case versus had no impact and how many you just get told no so it couldn't have an impact on the case?

NAOUM MENGLOUDIS

I didn't get the first part of your question, but for the second part, in our cyber unit, because we are very technical, we can discern between the cases and we ask for the specific information that we need. So, like, if we want a registrant's point of contact, we may have tried other ways, and we cannot do our investigation. So maybe sometimes it's the last resort because just the register of the domain name does not mean much. Most of the time, we look for WHOIS the administrator of the site, if there is some direct contact on the site, etc.

So, like most of the times, what we get helps us find our way through. But, for example, recently I remember a case with an MLAT, that because the judges are not very technical people, I don't know what they asked, we were looking for logs like IPs, etc., for a user, and they just give the registration information of the domain. Okay, maybe you can contact the owner of the domain and tell him, get your administrator to give us a date or something. But you can ask the first part again.

ROB GOLDING

How often do you find that you get a no initially and have to do the prosecutor's order versus you get assistance based on the first request?

NAOUM MENGOU DIS

Yes, it depends. In urgent cases, usually, we don't get a no if we can prove our case why it is urgent, etc. In child abuse cases, again, I cannot send you a screenshot of the content, but you can verify it yourself so there again there's more compliance. But in lesser offenses, for example, slander and simple offenses, of course, there should be like an prosecutor's order, and we will not go on without it because it's just legal stuff. For example, me personally, I don't give much weight on such cases because I deal with some more important cases.

MICHAELA SHAPIRO

Thank you so much. So I'm trying to remember the order again, right? I think, Sebastien, you had a comment, yeah?

SEBASTIEN DUCOS

Yeah, the way you described it, it sounds very complicated and very tricky. And I just want to bring back in perspective what you're asking us or what in general we're trying to do, not just with urgent requests and et cetera. If this process is not simple, and you put time pressure for us to answer, and then you hear Gabe saying, at least tell me no if that's what it's going to be because I need to hear it quickly, we're going to produce a no machine.

We can't handle complex things, particularly if we don't even have the legal backgrounds that you have, the legal protections that you have. So locally, it's easy because we know the local cops, and I understand that within Europe, it works well, within the United

States, it works well, but if you try to expand that around the world in that complexity with a bit of time pressure on it, it's going to be a no.

MICHAELA SHAPIRO

Reg first, and then Kristian? Is that okay?

REG LEVY

Thank you. Reg Levy from Tucows. I just sort of wanted to underscore that with a couple examples. If I get something from Gabe, I know what an FBI request, I know what an FBI request is, FBI warrant looks like, and I know how to look it up and validate it, and I know who to contact to do that. There are 16 states in Germany, and I have a company that needs to pay attention to the jurisdiction of Germany, and every state has a slightly different crest and way that they present their warrants.

Their warrants are far simpler, I call them warrants because that's how I treat them, but it's just a request from a law enforcement officer that references the specific law that they believe has been violated, then that is sufficient for a lot of data to be given to them. But I have run into multiple situations where those have been forgeries. So every single one that we get these days goes to my external counsel in Germany.

I live on the west coast of the United States, so if I get it at 9am when I first sit down at my desk, then maybe I still catch my attorneys when they are at work in Germany, and it's much more likely that I

don't get to it until 2 because it's not the first thing on my list of things to do, and then I'm not going to get their response until tomorrow morning. And so, again, these are complex issues, and we have run into situations where we've given domains away, we've suspended domains, we've violated people's privacy rights because of a forged law enforcement request.

MICHEALA SHAPIRO

Thank you so much. Noaum, go ahead.

NAOUM MENGOU DIS

Yes, thank you. Noaum, from Hellenic Police. For Sebastien's comment, yes, of course, like the proper ways to do it, the official channel, but most of the time we rely on your terms of service, as you mentioned earlier, like if we can just prove some evident abuse and we can get the information quickly, we're always trying to contact the provider first if we can get them quickly.

And then we may contact the foreign law enforcement via Interpol or Europol if they can get the evidence for us. And then the last resort is the MLAT, which will take about a year. I forgot what I wanted to say. Gabe can go, and I will come back to it.

GABRIEL ANDREWS

Yeah, this is probably more even towards Reg's comments, but yours were close. I think there is recognition that it's tremendously important to stop it when the criminals and the bad guys

impersonate the cops, like we all recognize that and we also recognize that. And we also recognize that it's work to address that problem, but thankfully I think we're already making some significant progress towards that in this space.

And this is something that we in the Public Safety Working Group are committed to doing our best to apply existing and aspirational tool sets that already exist out there to throw up this ICANN context, knowing that it will also be useful in other contexts outside of ICANN.

But we're actively working on better mechanisms to authenticate these law enforcement requests and make it easier to know, regardless of what you're going to say at the end, make it easier for you as a data holder to at least have faith and confidence that you are talking to who they claim to be.

MICHAELA SHAPIRO

Absolutely, but what I wanted to bring us back to is, and all of these are important perspectives to have in place, just one kind of perspective that we maybe haven't touched on quite as much is that of the registrant. So we have the perspective that we have to validate that these requests are in fact coming in. Then we then have the question of, well, what are the implications of disclosing this information?

And that's why, and I completely empathize with the perspective of the registries and registrars who are getting these requests. This is

an onerous process, but at the same time, we have to think about what the potential ramifications could be if that data is disclosed, because there are reasons, and this is something that Article 19 believes in very strongly, that you can't talk about freedom of expression without the right to privacy. One is kind of the flip side of the other, and more often than not, one is needed to promote the other and to ensure that it is upheld.

I do want to take moderator's privilege to maybe start getting into an interactive portion of the session. I really don't want to scare you guys off, but I promise this will be fun because the idea is that through role-playing a scenario, we're going to keep addressing these particular questions that have come up. Right now, we're in the theoretical. Let's try to bring it back. But I know there was one more comment that was in the queue. Did you still want to come in? I will turn to you before I kick it off.

HISHAM IBRAHIM

Yeah. Thanks for that. First of all, fascinating discussion, this is why I keep on jumping from the back up here. Hisham Ibrahim, again, RIPE NCC. Does or should nationality factor in here? To clarify my question, if a foreign police agency is asking for information pertaining to one of their own citizens, does that differ from if they're asking information from one of your citizens, asking information from a third country's citizen, and how do data protection laws and handling them factor in here? Sorry if it's a long question, I hope it's not.

MICHAELA SHAPIRO

Do any of the panelists want to come in on this? Yes, please go ahead, Reg.

REG LEVY

Thanks. Reg Levy, Tucows. Yes, absolutely. And I deal with this primarily with ccTLDs because law enforcement from Sweden asking about information for a .se domain, I'm going to treat differently than law enforcement from Sweden asking about a .com domain because it's more likely that it's directly relevant and necessary for them. I also want to address the comment from, I'm sorry, I forgot your name earlier, but terrorism tends to be one of the things that is on the urgent list, very important, the kind of thing that needs to be combated quickly and dealt with sensitively.

But in my experience providing data to law enforcement, one person's terrorist is another person's freedom fighter. And I managed to get caught up in the conflict between the Republic of Ambazonia and Cameroon, and the government in exile, which happened to be in California, so in my jurisdiction, had a domain name with us that the Cameroonian government was trying to suspend on the basis that it was terrorism.

I had never heard of this conflict before, I had to educate myself, but at the end of the day, I could rest on the fact that this was a U.S. citizen, the request was coming from Cameroon, and so I didn't have to even deal with it. So, there are all kinds of weird conflicts

that come into play, and we try to err on the right side, and we never know what that side is.

NAOUM MENGOU DIS

Yes, I'm coming back to Sebastien's comment, sorry. Yes, the best way is to have a direct cooperation with each company, but given that there are so many companies, I don't know how possible it is. For example, with all the major electronic service providers like Meta, Google, Microsoft, our cybercam unit has direct cooperation. For example, with Meta, years ago, we were on bilateral calls, and we figured out a formula how we can make our requests so they can comply with them.

And this included a specific order written a specific way from our prosecutor, like specifying some parts of our law and addressing Meta in a certain way. So we figured out a formula to work together more officially instead of going like the MLAT, etc. And I remember one of the big cases we had like a couple of years ago, there were some phishing sites, some GoDaddy fishing sites specifically, an MLAT was requested, of course, but you were very quick to give it to our friends in the US law enforcement, so we could get it, this way too so we managed to do our job.

MICHELE NEYLON

It's Michele again. Just briefly on Hisham's thing about nationality. I think your choice of wording is interesting. So do I care what nationality my customer in Ireland is? Do I even know, because

that's what you said? I care about the jurisdiction that I'm in, that I'm operating in. I think it's a bit like to Reg's point, it's impossible for me to know what kind of relationship they may or may not have. I mean, to be perfectly frank, I don't care. That's not my problem.

Their nationality isn't the thing, the jurisdiction that I have to deal with is. When it comes to ccTLDs and things like that, often the request will go to the ccTLD registry directly because the majority of them are thick registries. It's only when it's thin registry that it's likely to come to us. I could mention about IP addresses to get you all excited, but I'll leave that alone, maybe I'll throw in an AS number later. Thanks.

MICHAELA SHAPIRO

Thank you so much. No, and thank you all for these contributions. I think it's very clear that there's a lot more to be discussed on this topic, and what I hope we can do is through kind of role-playing a scenario, the kind of questions that come up as we play these characters, as we go through a situation that is hypothetical, but loosely based on the reality that we live in, that we can kind of start to continue uncovering these questions and continue moving forward in the discussion.

So I have a scenario, and I will read it out. I also have three very, very kind volunteers in the room who are each going to be playing a character. We have someone representing the registrant, the law enforcement perspective, and the registrar. So I'll read the scenario, and I'm happy to repeat it, and I realize I didn't have a

chance to send this slide over to Andrea, so at the moment I'll read it out, I can always repeat it, and please feel free to ask me to repeat any elements of this. But then I'll turn to my characters and ask them to potentially start acting this out. So thank you so much.

ANDREA GLANDON

Michaela, I can make you a co-host and you can share it if you'd like.

MICHAELA SHAPIRO

That would be lovely. Thank you so much.

ANDREA GLANDON

Great. Just a moment.

MICHAELA SHAPIRO

Fantastic. So we will actually have it on the board, but I'll still read it out loud because that's fun. So we have a human rights activist, they own a domain name, and on one of the websites through the domain name, she shares and documents human rights violations of the country in which she resides. During an uprising, a famous brand is a culprit of human rights abuse, which she mentions on her website using their logo.

For her own safety and privacy, she has remained anonymous on the website. A state actor wants to stop her from sharing this information, and they order the state's law enforcement agency to request the registrant's data from the registrar in order to track her

down. No bueno. So I would like to ask one of my intrepid volunteers, anyone who would like to go first, to kind of discuss who you'll be playing. Maybe I could turn to Clara.

CLARA LUDVIGSSON

Hi, I'm Clara Ludvigsson from the Swedish registry. Normally, at this point in this play, I'm very anonymous, I'd like to stay anonymous. I am the registrant, I'm a human rights activist.

MICHAELA SHAPIRO

Thank you so much. Yes, go ahead, Callum.

CALLUM HARVEY

Callum Harvey, Oxford University. I've been given the role of a state law enforcement agent. I've been ordered to obtain any information about this human rights activist by any means possible. So we'll see how that plays out, but I will be unrelenting, apparently.

MICHAELA SHAPIRO

Thank you so much. And my final volunteer.

LAILA LORENZON

Hi, everyone. My name is Laila. I'm from the NextGen, and my role is a registrar. So, yeah, I guess I would just like to ask more information about the request of law enforcement on the status and why this should be taken out.

MICHAELA SHAPIRO

Thank you so much. And I wonder if we could zoom in on the prompt itself just to have the scenario up there because we have our characters. Yep, right there, right there. There you have it. So I would love to start with a conversation between Clara and Callum, and that way it will be very short, just maybe you know what kind of concerns are you having in this moment, what would you want to ask one another, what would you say to one another, would you be excited to chat with one another, how would you play this out?

CLARA LUDVIGSSON

Well, I can start. I'm very happy that we speak. I'm very, very afraid because I fear for my life if my identity is revealed to the authorities. As you know, I have a very important webpage online that is very important, but my identity in this context is not important.

What is important is that we try to protect it. So I would like you to recognize my human rights to stay anonymous and not be subject to potential consequences that could involve torture in my home country. I would like you to keep my identity private and not disclose it to law enforcement.

CALLUM HARVEY

I can absolutely sort of understand elements of that. Boy, Micheala, you've been in such a great position. Thank you for this. In the interest of sort of public safety, things are occurring that could perhaps upset elements of social cohesion. While i can

appreciate that perspective, we do need that information and I would really like to just impress that it is not perhaps in the interest of one individual, there is a arguably a greater good piece at play here.

MICHAELA SHAPIRO

Thank you. And how about we bring in our last perspective? How would you want to come into this conversation?

LAILA LORENZON

Yes, so I think it would be important to assess the impact that this will have on the activists, so in case her identity got exposed, so what would be the consequence of that? Maybe law enforcement can help us with that.

MICHAELA SHAPIRO

Fantastic. What kind of questions would you want to ask? Or I guess where, maybe turning to law enforcement, how would you respond to that concern?

CALLUM HARVEY

I'm sorry, would you be able to repeat the concern, please?

LAILA LORENZON

Yes, thanks. So my question is, how would be the impact on this activist's life, his identity is disclosed, and also how you use this

information, maybe against her or on her? So what would be the steps you take to make sure that the make sure she will be safe?

MICHAELA SHAPIRO

Fantastic. And perhaps maybe Clara, do you have any particular questions that you'd want to ask from law enforcement? Is there a particular procedure that you would want them to have in place in terms of how they treat this kind of request for data?

CLARA LUDVIGSSON

Well, I would certainly want them to treat the request in a lawful and transparent manner that safeguards my human rights as an activist. Yeah.

MICHAELA SHAPIRO

Thank you. Any final comments from my beautiful volunteers?

CALLUM HARVEY

Absolutely, and we'd be looking to sort of any kind of rights governance frameworks and including a human rights assessment as well in the course of acquiring that information and making sure that it is bucketed in the correct way that it wouldn't then be used for other purposes potentially down the track as well.

MICHAELA SHAPIRO

Thank you so much. Can we have a round of applause for my volunteers? Thank you. And I know this was a bit gimmicky and I

know it's probably not aligned with real life per se, but I would love to turn to Reg who I think wanted to comment on this example.

REG LEVY

Thank you. Yes, I had a similar situation where I received a request for registrant data for a domain and the domain name itself, all of this was within jurisdiction, so local issues. The domain itself was something along the lines of governorjoeisterrible.TLD, and the request said we're in the middle of a gubernatorial election and I want to know who is behind this domain because I'm concerned about essentially fake news.

And I took a harder look at that than I would have at perhaps a different request because that, to me, seemed to implicate free speech, seems to implicate election issues, and other things. I actually reviewed the website, I went a little bit in-depth into the issues around Governor Joe and what may or may not have been at issue.

And in that case, I decided that it was not appropriate to disclose the information. In that case, although it was framed as a, this person is transmitted submitting fake news, it seemed more reasonable that this was someone trying to shut down somebody who was bad-mouthing or providing information to the public that they didn't want out there.

So not analogous exactly, but a similar sort of situation where I felt that free speech rights and, again, election rights were being

implicated, involved in the request, and that the person who owned the domain might be at risk if I did disclose the information.

MICHAELA SHAPIRO

Thank you so much, Reg. I really appreciate it. Yes, I see a hand down there.

ROB GOLDING

Rob Golding, for the record. Within that scenario, you end up with the reality, and I hate it when reality gets in the way of life, that a lot of this potentially can come down to making the registrar morality police, that they have that final decision, it's either left with a member of staff to decide or it's left with policy to decide, or it's potentially even management's life, limb, and liberty or their business, people will generally cave under that, they will give out the details because they have to protect the people they have to protect, they have to protect Reg if she works for Tucows.

They wouldn't say Reg has to go to jail because she's protected even if the details are true even if the details are verifiably correct. And if you're going to make the registrar the morality police, I think the world is in serious danger.

MICHAELA SHAPIRO

Yeah, I would completely agree. We tend to stand on the position as Article 19 that infrastructure providers are not the, what's the word, arbiters of justice. While you guys do fantastic work, I don't

think that we need to add to your to-do list. But I think this question has gotten a lot of excitement, so I'll turn to Reg, and then I think Michele wanted to come in and then Gabe.

REG LEVY

Sorry, Michele, panelists privileged here, jumping the queue. Rob, I would submit to you that that is always the case, and that at the end of the day, registrars, any business, needs to make a decision about how it's going to conduct itself and what its own morals are, because relying on, oh, well, just the letter of the law is one position, and it could protect one side, skirting the other the edge of the law might protect another side, and every registrar and every employee at that registrar is going to need to make a decision about what they think in each case.

And I tell my people all the time that I will stand behind their decisions, because a lot of these are hard decisions, and there's not often a right answer. So if one of my direct reports makes a call that I disagree with, that I would have made the opposite call, we'll stand by that call because these are hard questions. And often in the Slack channel that nobody else at the company gets to see, we discuss these. Like, here's a situation, what would you guys do? And we at least talk it out, because every single one of us is a moral being, and every single one of us has to make decisions based on what we can sleep with.

MICHELE NEYLON

Thanks. Michele for the record, again. I suppose another thing is that we sometimes guess what we would consider to be quite frivolous reports of various different times. They're looking for us to take some kind of action either disclosing information or taking action. And in many cases, the situation is some kind of fraud, some kind of alleged criminal activity, but the request is coming to us from some random person.

So, we tend to do is to say, well, actually, go-to law enforcement because we assume that law enforcement will actually do what it's meant to do, and then once we get a request from law enforcement, then we may or may not act, but at least that way, it's being handled sanely. I am not the internet police, I definitely do not want to be the moral police, so it makes my job a lot easier if I'm able to say we did this because on Garda Síochána, which is the Irish police, following proper procedure, sent us a proper request to do it, as opposed to, I took something down because some random guy sent me an email saying that he didn't like some content on a website.

So in that respect, I think it's important to not look always at the police as being the enemy. They can also be the ones who actually are able to say, well, no, this request is ridiculous, it doesn't meet any standards for anything.

MICHAELA SHAPIRO

Gabe, did you want to come in?

GABRIEL ANDREWS

So, I found this conversation to be pretty interesting. Going back to the scenario you had, it was creative. I thought the use of the intellectual property handbag in it was sort of a twist I never contemplated before. But I wanted to add just some real old experience because I have not often in my career dealt with human rights agencies, but there was one occasion that I'm reminded of now when we have this example, and it's been a few years.

But there was an instance where you know as a U.S.-based law enforcement officer I was given from another office a list of, I forget, somewhere around 8 to 12 out of LA, so 8 to 12 human rights agencies that were in the LA and surrounding area that had been targeted by a particular foreign government and that they had all been the recipients of phishing messages that we knew to contain malware and that these would install key loggers and so on and so forth and compromise networks. And so it was my job to basically figure out, okay, well, how do I let each of those entities know?

And just to flag, this is one reason why I think it can be quite valid to contemplate which nations you're speaking to because now you're talking about one nation is trying to help the human rights agencies and one nation was very much targeting them. And so what I ended up doing is at that time, yes, I did use things like WHOIS data to find the technical and abuse points of contact that were associated with the domain names that they used in the in the victim email addresses when that was relevant, but some of them

might have used Google too right you know then that might also be not available to me.

But just to highlight that it can cut both ways, I totally understand that disclosure of data when you're trying to remain anonymous is absolutely something that you'd be concerned with, and quite conversely, sometimes your local law enforcement's ability to obtain that same data might actually end up protecting you, and it all comes down to the circumstances.

MICHAELA SHAPIRO

Thank you so much, Gabe. Do you want to come in?

FARZANEH BADIEI

So this is a very interesting conversation, but I just wanted to kind of talk about the human rights framework that registrars and registries in the case of ccTLDs can actually use when they don't have a framework that they can, like a legal framework. And this is where our work comes in. We can come up with processes and steps that you can follow in order to see how you should make that decision.

And one thing that Hisham has been mentioning which I think is very important is that not all law enforcement is as nice and shiny, and they don't have the processes in place, they don't get audited, and there can be severe human rights implications. But a registrar that is not in that country, that does not have a good understanding of what is going on, might be able to use this human rights

framework to make a decision that could potentially protect that domain name registrant or reduce the human rights impact. Also, when it comes to ICANN, I'm going to talk about my revolutionary ideas later.

MICHAELA SHAPIRO

No, what I wanted to comment on first is to thank you all for being so engaging. This has been so much fun for me. So thank you, selfishly. But I did want to come back to a couple of points that I feel like have been kind of trending across the panelists' responses, which is incredible. So both the importance of contextualization, the importance of the relationships with local law enforcement, that keeps coming up in this discussion.

I also wanted to come back to a really great point that Reg mentioned about the complexity of these decisions and I think you mentioned there was some discussions that you have internally to when you have a particularly tricky case, and I wonder if there's a way I understand that there's obviously we can't do this on a macro level on specific cases but I wonder if there's best practices and guidelines that we could come up with that it's like when I came up with this type of particularly tricky case as registrar A, this is what I did, and registrar B could really benefit from this because they're also facing a similar type of issue.

So I wonder it's something that Farzan and I have tried to do in kind of the DNS abuse context is come up with tools and frameworks to address as I think as Sebastien who mentioned earlier the kind of

the volume issue and the urgency issue and how do we do this in a quick but efficient but right to respecting way which is it always keeps coming down to that. And just the last point going to what Gabe was talking about that example I thought was fantastic because it also brings into place or it contextualizes the discussions we're also having in all other arenas within ICANN about DNS abuse and how do we mitigate this and the ramifications that that could have if it's not addressed.

And so what I've would love to have happen after the session is for all of us to come away with things that we could do together to compile some of these ideas. And so that's what I'm planning to do at least when I watch the recording again. But what with the time that we have left, we have eight minutes, so as moderator privilege, I want to take let's see, maybe three minutes to open up the floor. If anyone who hasn't spoken yet and maybe isn't even sitting at this table or is and has a question because I know we have a multi-stakeholder process for a reason, and I would love to hear from others who maybe haven't had a chance to come in yet. I see a hand down there, so please do go ahead.

BRUCE TONKIN

Hi, thank you. My name is Bruce Tonkin from .au. Just another element that I haven't really heard mentioned in the room so far, but the basic scenario you put forward is there's some sort of offending content, and we need to release information about the registrant to the law enforcement. What we see in .au quite often

is that the websites that hold some sort of offending content have been compromised, so they've been hacked essentially. And so normally in those scenarios, we would be contacting the registrant using the information we have and getting them to remove the offending content which they're usually happy to do.

Providing the information about the registrant to the law enforcement would then have quite a high bar for that law enforcement agency to get that information. But often the real issue is getting rid of the offending content. So just something to think about. So that is perhaps a step first, which is, is there an opportunity to remove the content first?

Maybe that's a bit complicated in some of the human rights scenarios, but often if you de-escalate the situation, us contacting the registrant, getting the content removed, and then you can use more substantial processes to request the information which might be through the local law enforcement body et cetera, if you really do want to proceed to prosecution.

MICHAELA SHAPIRO

Sorry, I'll come in on that. Just to say when it comes to content, I do think that is another can of worms that we can certainly open in a future session, but as a quick response I would say when it comes to removals or requests to take down specific content, as a position from Article 19 side is we don't see the registry and registrar as the

right entity to go for content removal. That's a blunt force tool, it can't target a particular web page unless I'm misunderstanding.

BRUCE TONKIN

No, I'm saying the registrant removes the content.

MICHAELA SHAPIRO

No, understandable. Thank you. Well, I would love to have Farzaneh wrap up. I also would love to take advantage of my panelists here who are so brilliant. And if in one sentence, you could let us know, one thing that you'd like the audience to take away from this session. What is one thing that you think people should know about this topic or one recommendation that you have? So I'd love to maybe turn to Reg to kick us off and then we'll go down the line.

REG LEVY

I would say that these are issues that registrars are constantly thinking about. We may not necessarily couch them in terms of a Human Rights Impact Assessment, and we may not go through all of the steps that we learned in previous HRIA sessions, but we're always considering the impact of our decisions on our customers, on the potential victims, and on the requesters.

NAOUM MENGODIS

Yes, thank you. I would like to say that police is not always the bad guy and we deal with other people's problems usually, and

sometimes the law is just the law and we have to do some processes.

KRISTIAN ØRMEN

Like I mentioned earlier, that we sometimes get a lot of heat for saying no many times, but I think it's important to note that we, of course, care about abuse, and we are aware that registrant data can sometimes be important in solving abuse cases, but we also have to protect our registrants, and in each case, we have to look at both sides of the case for taking a decision.

FARZANEH BADIEI

Okay, so thank you so much, everybody. Thank you so much, Michaela, for bringing your expertise and human rights here as well. And so this is a first step for much longer conversation about how these issues are going to play out at ICANN because we might have some... there are some policies that might come into effect that there might have some disclosure implications, and it would be good to be ready to come up with best practices on how to follow human rights principles, but at the same time disclose the registrant or make a decision about disclosure of domain name registrant data.

Through these scenarios, as we are trying to clarify what we are talking about when we say that these decisions have human rights implications. And also we want to be helpful to the community, to the requester community as well, to when they submit these

requests to have processes themselves that can hold them accountable, that can be transparent and also bring more transparency in general to this system.

So for the next steps that we can, the Non-Commercial Stakeholder Group will also like work with other stakeholders to discuss these issues, and hopefully we will come up with some guidelines on how to do our work and respect human rights at the same time. Thank you so much for attending.

ANDREA GLANDON

Thank you. You can stop the recording.

[END OF TRANSCRIPTION]