ICANN84 | AGM – GNSO: DNS Security Without Sacrificing Rights-HRIA on RDRS
Saturday, October 25, 2025 – 13:15 to 14:30 IST

ANDREA GLANDON

Hello, and welcome to the DNS Security Without Sacrificing Rights, HRIA on RDRS session. Please note that this session is being recorded and is governed by the ICANN Community Participant Code of Conduct, ICANN Expected Standards of Behavior, and the ICANN Community Anti-Harassment Policy. Please observe the following guidelines to participate in this session. I will also post them in the chat for your reference.

Only questions posted in the Zoom chat identified as a question will be read aloud during this session as time permits and when directed by the chair of this session. If you wish to speak, please raise your hand in Zoom or otherwise as directed. When speaking, please state your name for the record and speak clearly at a moderate pace. And I will now hand the floor over to Rafik Damak, the NCSG chair. You may begin.

RAFIK DAMAK

Thanks, Andrea, and thanks to everyone who is joining us for today's session, and I hope you enjoyed your lunch. So, this session, which is about the Human Rights Impact Assessment of RDRS, it's basically a follow-up of several sessions that we had about the HRI to cover different aspects. And for today, we will focus on RDRS. And with that, I will hand over to Farzaneh Badiei,

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.

who will moderate this session and will give us more overview about the purpose and what we will discuss today.

FARZANEH BADIEI Thank you, Rafik. Hello, everybody. So, this is one of our standard Human Rights Impact Assessment sessions that NCSG has started doing since beginning of the year. And for each session, we decide on what sort of ICANN initiative we want to focus on and discuss with the community on the potential Human Rights impact of the projects and the pilot projects that they have.

This session is about RDRS. I think everybody kind of knows what RDRS is. RDRS is the pilot project for the triage of the request to the domain name registrar and private sensitive data. And it's being run by ICANN. It's a pilot project. And it's at the end of the two years, I think. And it's voluntary to opt-in for the registrars. And now we are at the end of it and we are deciding on the next steps. If we can go to the next slide.

So, as I mentioned, the goal is to-- So, it's not a disclosure system as such. The goal is to streamline communication between requester, law enforcement, IP holders, and registrars. It's voluntary participation by registrars in the pilot phase.

Next slide, Andrea. So, why does this even matter for Human Rights? Because there is no direct disclosure. Why are we making a fuss about this? So, one of the reasons that it involves, and somehow, at some point, involves disclosure of data to the

requester. So, when the registrar considers it, will make a decision on whether to disclose the data or not, which can have an impact on privacy, freedom of expression, and access. Decisions about access to private data, even if it's like a triage system of the request, can have an effect on security of users, journalists, activists, and people who we care about at NCSG.

Next slide. So, at NCSG, we are not against standardization of request process. We believe that it brings predictability to data request handling. It creates transparency around how data is requested, and which stakeholder, which requester, is it the IP holder, is it law enforcement? Helps establish some kind of accountability mechanism, such as authentication of the requester, which RDRS does not do at the moment. But we are hoping that it happens at some point.

And can encourage Human Rights-based processes, like documentation, reviews. So, on its own, RDRS, in my opinion, is not. Actually, can bring more transparency. For example, if you look at the reports that are done by RDRS, for example, we have how many requests are from law enforcement, where are they based. We have the number of requests from IP community.

So, we can have a general picture of where these requests are coming from, which is something that we didn't have before. There are certain registrars that have transparency reports, but it's not overall. Not everybody does it. So, with this aspect, we are good with that. There might be an ugly part to it, though. Next slide.

So, one of the reasons that it can impact Human Rights is that if RDRS becomes mandatory, registrars might feel pressure to disclose private data automatically, rather than evaluate the necessity, skip Human Rights review of individual requests, and normalize over-disclosure or mission creep in data access. So, we think that a voluntary system could work, but if we make it mandatory, it will need to have more transparency and accountability mechanisms in place.

Next slide. Oh, that's it? Great. So, now, I have two speakers here. Now that I told you all about the Human Rights aspect and the accountability aspect, I have Reg Levy from Tucows. Reg can tell us a little bit about their experience with the triage system and obstacles to standardization and how you generally do process the data request. Maybe you can also touch upon why you opted out of RDRS. And then we have Alan Woods from CleanDNS, which Alan will touch upon mitigating DNS Abuse without encroaching on Human Rights and without disclosure of--

What are the alternatives to disclosure of private sensitive data in order to bring security? So, with that, I go to Reg to discuss. Yes, go ahead, Reg.

REG LEVY This is Reg Levy from Tucows. Next slide, please. So, I used the Tucows form for these slides because I want to be clear that this is my perspective. This is how I and how Tucows approaches the

RDRS, but it's not going to be the same necessarily for every single registrar. And you're already on the next slide.

ANDREA GLANDON Reg, I'm sorry. Can I just have you get a little closer to the mic? It's a little hard to hear you.

REG LEVY I'm not allowed to move the mic.

ANDREA GLANDON No. Thank you. Let's see if that's better.

REG LEVY Check, check.

ANDREA GLANDON Much better.

REG LEVY Thank you. Okay. This is Reg Levy from Tucows. I'm not going to repeat all of that. Okay, so in the first instance, we look at the request that has been received. When you guys get these slides from the website, you will see that this is a link to the Registrar Stakeholder Group recommended minimum required information for WHOIS data requests. And I'm going to have a bit of a summary on the next slide, please.

So first of all, we need to know who you are because we are going to be disclosing personal information to someone. We're not disclosing it to an organization. We're not disclosing it to an anonymous person on the internet. We need to know who you are. We built a system that will automatically disclose who has requested the information to the data subject. So, this is also part of why we need this information, because they need this information and they deserve to know who has access to their data.

I also need to know what domain you're asking about. And that sounds like a baseline requirement, but you would be surprised at how often that is omitted or how often people just say, no, I need access to your WHOIS database. This is a per domain evaluation of each person's requests and the merits of the request itself, which goes on to your legitimate interest. Tell me everything that you think is relevant to why you want this information.

And in the next column, we have an assurance that this is a need that you actually have. So, not just what your interest in the data is, but you cannot accomplish that interest without the data. Those go hand in hand.

Part of that is requiring that if you represent someone, they know that you represent them. Again, this sounds like it might be a baseline assumption, but we have received competing demands purporting to represent the same entity with regard to a single domain. And at that point, I feel like someone, somewhere there is

a disconnect. And so, I don't want to release, again, personally sensitive information.

The name and address of a human being to two companies representing a third company and none of them actually knows what they're doing or that the other one is doing it. We also want an assurance that you understand that this is a person's information, that you are accepting all of the legal and moral responsibilities of treating that data with the sensitivity that it deserves. And then we, in a way to keep honest people honest, we ask that you didn't lie or misrepresent. Next slide, please.

RDRS is, and this goes toward why we ended up opting out of it, it is an operationalization of the document that I linked to two slides ago of the minimum data requirements questionnaire. We have found that turning that into just a set of click-throughs like, yeah, I agree, I agree, I agree, I agree. It invites casualness and a way for people to say, to not read what the, pardon me, to not read the piece that says, yeah, I didn't lie. Yeah, this is what I think. Yeah, I thought clearly and I thought about this before I, you know, I wrote it down. I made the request.

We're all used to click-through agreements. Nobody reads the terms and conditions for anything. So when you operationalize a system like this that, again, affects people's data, I have found that it invites a sort of a sense of casualness with regard to the requests and therefore with regard to that data. So, that's part of why we ended up opting out. I know I did these backwards.

In addition, bulk requests are typically not feasible. The information that you require for domain.tld is very rarely exactly the same reasons that you require the information for domain2.tld or domain.tld2. In some cases, there is overlap and so we have entertained in the past similar or single requests for a handful of domains. But in general, we have not found that allowing for bulk requests adequately protects the rights of the registrant. Next slide, please.

WHOIS privacy tends to be a question with regard to RDRS. People are welcome to make requests for domains that have who is privacy enabled through RDRS. We consider that who is privacy, that the information underlying who is privacy are company records and that those are protected by due process. So, we are happy to entertain requests through RDRS as long as the appropriate warrant or subpoena is attached.

Next slide, please. We also run into a number of jurisdictional issues. I'm sure that everybody here trusts their own government with their data. But does everyone trust every other government? The internet is global and part of the balancing test when we receive an RDRS request is the jurisdiction of the requester and the jurisdiction of the registrant and the jurisdiction of the registrar, which goes back to this is how Tucows approaches it.

It's not necessarily nor are we saying that everybody should approach it in this way. But generally speaking, we will treat requests from local law enforcement differently than we treat

requests from foreign law enforcement. And I hope that that is not a controversial statement. And if it is, I would love to talk to people who think that I should treat all law enforcement similarly. I'm not going to say next slide, please, because I think I'm just handing it over to Alan now.

ALAN WOODS Thank you very much. Alan Woods for the record from CleanDNS, and from for those of you not familiar with CleanDNS, we are an anti-online abuse, anti-online harm company and we work with a lot of registries and a lot of registrars doing DNS Abuse mitigation for them primarily and trying to branch out and hopefully work with other peoples on some broader harms.

So when Farzi asked me to do this, it was very much from the point of view of our perspective of how do we deal with the one answer that you seem to always get throughout the years when it came to dealing with DNS Abuse and release of registrant data when it comes to DNS Abuse. And I suppose CleanDNS was lucky enough because we're relatively new as a company, four to five years old, and therefore the challenge for us at the beginning was to understand the way data was being used in the world at the time.

The restrictions that were being placed on us for PII and in particular, how do we create a system by which we are not reliant on that sort of PII in order to do our job? And that is to quickly and accurately and respecting due process deal with DNS Abuse. So, that was where we started from. And those of you familiar with the

GDPR as being kind of the high watermark, it is the concept of privacy by default and privacy by design. That is how we started off. We said we have a job to do, but can we do this without reliance on personal data as much as possible.

So, the way I look at it and the way we always look at it, and I'm looking around the room and I'm not going to ding people up because I don't want to because this was very positive, but it would be unfair of me to say this. One of our particular clients at the moment put us through the rigour when we started with them about data protection and about how do you treat the data that we will send to you, as I nod to the person. And it was wonderful because it made me internally even think, how do I consider the data that we use?

And when you boil it down, how we consider the data that we do use, because there is times where registrant data will have to come to us. Say, for instance, if we were escalating to a registrant to say, hey, there's something wrong with your domain, please look into this. So, our point of view is that every single time we use registrant data, it is almost a request of our client. Can you provide that data to us? We did data protection impact assessments in order to assess in what time, what necessity would we have for that data?

So, one of those necessities that we come up with is, well, obviously, if I need to escalate to the registrant for a matter that they should know about, that is something that we would be able to do. So, we do not take wholesale registrant data in order to

review it back, left, right and up and down. What we do is we take the data when there is a credible report. So, when there is a report of abuse, only then will we seek the data if it is necessary.

So, that is where we started from. It is very much, as I said, privacy by default in the sense of we do not have the necessity. We use other indicators, infrastructure indicators, publicly accessible indicators such as screenshots, other indicators that are pointing to the fact that an abusive activity is occurring. And we rely on that and we are able to seek out other ones because of those indicators. And that's something I'll talk about in a second. Which then kind of so that's where we started from and we've continued on with that and again with the help of other with our clients have been very helpful in guiding our hand in that as well.

Now, let's look to the future a little bit and we are on the cusp of perhaps the new PDPs and one of them, of course, is the associated domain check. Now, that is one thing that we need to start thinking about. Well, how is an associated domain check when it's coming from an ICANN policy point of view going to affect the role of every party again in this instance? And for those of you who were part of the PDP on the registration data policy. Yes, I know I rolls all over. There was one of the major issues was trying to figure out who was a controller.

And so, I'm not giving advice. I no longer need to do that, thank God. But I'm in the place where I can say one of the cautions that needs to be taken into account, especially when we're talking

about things such as DNS Abuse and something as practical and as it makes sense as an associated domain check is in the policy to steer very clear of the concept of telling you what you need to do in that associated domain check.

Saying there was one as necessary is fine, but saying you need to check the registrant data and to check on that, you're putting a particular corporation into a controllership role because you're enforcing it in the contract. And I think you need to be very clear when you're pushing through that. However, there is something that I would like to think about.

And again, when we're talking about Human Rights impact assessments as well, specifically in this, we've had an awful lot of discussion about dealing with DNS Abuse, dealing with harms, and people may roll their eyes when I say this, but there is now an argument that we are more mature in how we're approaching this when it comes to DNS Abuse. And when it comes to looking at not just reactive mitigation, but looking at the proactive mitigation, which, you know, can be difficult.

However, in that context where you have unwell evidenced claim of abuse against a domain or two domains and there is an associated domain check, there is a point in which you have to ask the question of, is the registrant information here actually PII? Because if you think about the definition of what personal data is, is that it is data which identifies or is capable of identifying a real person.

Is at what point as the evidential thresholds established that say, well, now I'm establishing that this is more than likely not a real person and therefore it is data that should be considered. I don't want to say fair game, but it is data that should be considered as somewhat less protected.

Now, that being said, a Human Rights data or Impact Assessment, a data protection Impact Assessment, it's never perfect. You need to think about the data that you're using. So, if you are seeding data from an evidenced case of DNS Abuse, is that registrant data, which is very capable of potentially proactively helping with registrars and registries and dealing with abuse, is that data something that you could be able to use less restrictively? And I think the answer is with the proper paperwork, with the proper thought processes, with the proper assessment in place. Yes, absolutely.

So, from CleanDNS' point of view, that's something we're definitely looking into in advance of this. But in fact, mini plug, we're actually launching a new product called Pivot, which one of the things will be where we have data that is registrant data, but it's also infrastructure data. It's also everything underlying it. But can we see the patterns? Can we see where potentially there is DNS Abuse? And then can we seek out the evidence in order to move that forward? So, I think as we look to the future, I mean, I would suggest that caution is involved with this, definitely. But also, we were very scared of the GDPR and rightly so.

There are huge, huge fines. There are huge operational issues with this. But as we move to the next stage in our maturity and how to deal with this, I think there is a we should think about a be careful in the wording that we're using for the new PDPs, but also, we should be more willing to establish, to set out our camp and say, this is what we believe is good for data. This is the reasoning behind it. This is the Impact Assessment, both data protection and Human Rights and balance as well the impact of victims against the impact to the actual data protection or data subject rights of a potentially not data subject.

So, this new frontier, I think there was some very interesting and probably exciting conversations to be had when it comes to dealing with DNS Abuse and online harms, generally speaking. But what I would suggest is it has to be done with caution and it has to be done in the right place. And again, I use this in a blog post actually during the week, but like it since we're in Ireland, there's an Irish proverb, which is to slap to my Latin Hebrew, which means I love the Michele looking at me, which is a good start is half the work.

We are at the point now where if we start, well, thinking about privacy by design, thinking about privacy by default, as we go into this PDP process, it will take out some of the contention and I think we'll make a much better policy at the end of the day. So, that's my two cents, maybe 17 cents.

FARZANEH BADIEI Thank you. I see Sarah's hand is up.

SARAH WYLD Thank you. Hi, this is Sarah Wyld from the Registrar Stakeholder Group, I have two comments and a question for Alan. Okay, I'm going to go in backwards order of what you said for fun. So, I like that you're talking about doing a data protection Impact Assessment as well as a Human Rights Impact Assessment. I think both are useful.

They have different perspectives and approaches. And so, I think both should be done for all PDPs that include registration data or personal data in any way. And the public comment submitted by now, I can't remember if it was both the registrars and the Tucows comment or only one of them did propose that a DPIA should also be considered for those PDPs.

Next thought, you had suggested that maybe personal data, if it's used for well evidenced cases of abuse and probably doesn't identify a real person, could be processed less restrictively. And I agree, but I think that maybe that's it's not making an exception because it's not real personal data. I think it's a valid processing activity under the GDPR, regardless of whether the data is real or not, once the well evidenced report has been understood.

And my question, you had mentioned at the beginning that you rarely require registrant data, you might use it if you need to tell the registrant that they have a problem. Is that really the only time you

would be using it or are there others that should also be considered in the abuse mitigation context? Thank you.

ALAN WOODS

Thank you very much. So, to answer, well, to actually answer questions that you didn't ask and then I'll answer your question. So, the first one was when you were talking about it being in line with an actual legitimate data processing under the GDPR. I agree. And there's also a little known or little used recital and I can't remember the exact recital now, but it is on information security, in effect, data processing for information security purposes. And I think that's something that we need to consider a little bit more. And I think it's something that, you know, it's not a safety in numbers thing. It's about, as I said, setting out your camp and fighting your point, because I think we're at the point now where we know maybe a lot of the pitfalls and work through that. So, thank you, I agree.

To answer your question then, yes, one of the things that we do in CleanDNS now is we also have sinkholes. So, instead of just putting domains on a server hold or a client hold, we're asking clients if at all possible to put that domain into a sinkhole. So, even though it's not registrant data, there is a lot of data that can be used in order that could be considered personal data in that as well. And the ever present concept of the IP address is that personal data, is it not?

And I think remembering the European Court of Justices rulings where they say, as long as-- you know, IP address is PII. And I'm

being very, very-- actual real lawyers in the room will probably give that to me for saying this, but basically what they're saying is that if you do not have the data that can link that specifically to that person, then there's less of a implication that it is PII in the truest sense. That's a real bad way of putting it. But, you know, the safeguards are still must be in place, but you can use that data legitimately as probably a lower bar in order to prove that.

So, yes, there is always going to be elements of PII that I think we need to use and could use and used to great effect. But again, it's don't put the cart before the horse. That's we need to ensure we need to know what we're doing and when it comes to tasks, because this should be open, this should be transparent and we should be able to explain why we are processing the data, not after the fact, not after the questions being asked, but before you start processing that data.

FARZANEH BADIEI Thank you. And Thomas.

THOMAS RICKERT Thanks so much, Farzaneh, Thomas Rickert for the record, representing the ECO Association. Thank you so much for putting this meeting together. I think that's very important. I think it would have deserved more audience than we have in the room today. But I think based on what Alan said with the upcoming policy development processes and other issues, you know, we should

maybe push for having a bigger meeting where, you know, we have a town hall type thing to discuss Privacy and Human Rights related issues with respect to the policies and the services that ICANN is developing.

Now, I think we're having or we should probably make a distinction between two different discussions. One is the DNS Abuse mitigation, where we're moving more and more towards mitigating abuse without needing the PII to support it. Although some want to make us believe that you need to you need the PII for everything. And I think we need to push back on that particularly since the temporary specification came into place, a lot of affected parties, but also the service providers that help them with abuse mitigation found ways to very effectively address abuse without knowing who the registrant is.

The other aspect, and I guess this is the focus of today's discussion is what about registrant data that is allegedly needed or needed to carry out investigations to find underlying crimes, to find the perpetrators. And I think that just to, you know you will hear me talk about a lot of hesitations with this but this is an important part because the reason why we see so much cyber crime these days is because hardly ever is a perpetrator caught and held accountable.

So, that is an important thing, but we need to get it right. And it looks like Reg has intentionally kept that slide up for me because I want to point to the jurisdictional aspect of things. And Reg, you

said that probably a tongue in cheek comment that you trust your local government.

In my legal practice, I've seen so many I'm not sure what the English word for that is crappy law enforcement requests that, you know you should be very careful even disclosing to your local law enforcement authorities. And that's an issue that we hardly discuss ever at ICANN. I don't know why, you know, we've brought this up multiple times over the years but it doesn't seem to get traction.

So, we have finally started a discussion on this in the GNSO of council. I will also report on that during the joint GNSO of council and GAC meeting tomorrow, but the RDRS as well as the new registration data policy are read by some like it's a highway to getting access to data. And there's no promise in the RDRS that you actually get data.

It's a matching facility to get requestors in touch with the contracted party that holds the data but then the real work starts. And, you know, I've been sitting in these meetings and heard requests for automated decision. You know, you shouldn't make any assessments but data should be disclosed in split seconds that all sounds nice and reads well on paper but don't take it from me, take it from the European Data Protection Board that has issued guidance. It's guidance two out of 2024.

It was published this June, which is why it's very recent and pretty comprehensive. It's an excellent read because what it basically says is if you talk about cross border disclosure requests and if it's

between two countries where there's an MLAT treaty in place the default response from a company should be refuse, decline, right? That doesn't mean that that's the end of the story.

So, you can then go through the entire catalog of the legal basis in article six of the GDPR if you want to look that up but the European Data Protection Board says that's to be done on a case by case assessment. So, you can do it for life and danger for individuals. You can do it in other cases of urgency but you need to be very diligent. And in order to pass that threshold, some work might need to be done.

Then, the law enforcement authority and the requesting company where there's an MLAT treaty in place should go to the local law enforcement authority and they can then ask the contracted party. So, if you're receiving a request the European Data Protection Board says tell them to go use the proper process, go through the local law enforcement authority.

Then we have this new trend whereby international agreements are negotiated and laws are being made whereby law enforcement authorities from other jurisdictions can directly request information from an entity. That is true for the e-evidence regulation that's going to come into force next year. Operationally that's going to be a little bit of a nightmare because you only have a limited catalog of reasons to refuse. Then we have the second additional protocol to the Cybercrime Convention or Budapest Convention as it's also called, but that has not yet been ratified. So,

that's not yet there but that also deals with disclosure by private entities.

So, there's something coming up but we don't have these tools right now. And therefore, I think we should tell the rest of the world that if folks paint the RDRS as not functioning because the disclosure rates are too little that may also be the case because there are jurisdictional hurdles. And we should have a discussion with the law enforcement and the government community to talk about these things.

And we should talk about how to get it right. I'm not against disclosure, but as we've heard previously it needs to be done correctly. The rights of the data subject whose data is concerned need to be balanced appropriately against the rights of those who are requesting the data.

So I hope that this is part of a pivotal point where we can actually have these discussions to talk about the legal instruments that we're potentially missing that we need in order to make this work better. And also, to make sure that those who are asking for data and don't get it are not disappointed if we're just doing the right thing by declining disclosure.

FARZANEH BADIEI Thank you for that, Thomas. I want to build on a couple of things that you mentioned and I know that I'm jumping the queue. So, thank you to the chair for letting me do so as a panellist. I do think

that talking about our DRS and data disclosure is distinct from, and we should not conflate it with any type of DNS Abuse mitigation. That's a wholly separate topic. That said, with regard to due process and MLAT treaties, I have seen a disturbing trend within ICANN that is trying to chip away at due process by circumventing it through ICANN processes.

If our contract requires disclosure of data in a certain instance, that means that we and that our customers no longer have the protection of due process. And due process is different in different countries. And a refrain that I hear from law enforcement in my daily job as well as at ICANN is that due process is hard. And MLATs are really annoying and slow and difficult. And boy, wouldn't it just be better if you just gave us all of the data? And no, that due process is hard, that's correct. It is a Human Right and we need to stand up and protect it. So, we have quite a queue here. We have Michele.

MICHELE NEYLON Thanks. Michele for the record. Okay, so this is meant to be around the RDRS and Human Rights and the Human Rights Impact Assessment. So, kind of taking that back a little bit. I mean, first off, I think we really do need to put a marker down with ICANN. All PDPs should include a Human Rights Impact Assessment. Security, stability, Human Rights. It's not particularly complicated. It's just a bloody checkbox. You check, you see, does it have an impact?

And that leads to the other thing around the data because obviously some policies are very obtuse and don't really involve anything real. Others are very, very real and do involve lots of things that could be all sorts of problematic. And just to back up Reg's point, I am sick to my teeth of this rubbish where ICANN believes that it can write policies and put things into contracts that somehow completely ignore due process and local law.

There is no reality in which you can force Angar Deshi Akana to go and register with some weird ass system being run by a not-for-profit in a totally different jurisdiction. That's not going to happen. Angar Deshi Akana will literally send a squad car to my office and sometimes when they're feeling in a particularly nasty mood, they will wear their anti-riot gear type combats. No, no, they've done this, Alan, believe me. I think that might've been coming from something else, but they literally turned up wearing the flak jackets. It was the most ridiculous thing ever.

This is for a data request, it was hilarious. But there is no reality in which you can say, oh, you must use this kind of system to talk to law enforcement, or you must use this system to talk to somebody else. That's not how reality works. It really isn't. Also, it's really disturbing to hear that the ICANN Board wants to turn a voluntary system that a lot of the registrars who did voluntarily agree to engage with, they're trying to turn a voluntary system that's already been proven not to be particularly useful, trying to make it into an obligatory system.

Now, last time I checked, the ICANN Board sits at the top of the multi-stakeholder model. And since it's meant to be bottom-up policymaking, how is policy being mandated by the Board bottom-up? If somebody can explain that to me, maybe I misunderstood how gravity works. Thanks.

FARZANEH BADIEI: You all are doing such an amazing job for having an engaging session. Thank you. Michaela.

MICHAELA SHAPIRO: Thank you. Michaela, for the record. Hard acts to follow. So, thank you so much, everyone, for making my input quite easy. But I wanted to come back to, there was a question that came from Sarah earlier about, and it's building on some of the comments that were made earlier, distinguishing between HRIAs and data protection HRIAs, or I forget the exact terminology there, but I think for me, when I think about Human Rights impact assessments, that tends to generally cover elements of data protection and privacy.

So I'm just curious how, if perhaps that's maybe my misunderstanding, or if there's different ways that those in the room are conducting those kinds of evaluations, if there's different criterion that you're specifically focusing on when you do a specific data protection evaluation versus just a broader HRIA. And that can kind of go to anyone who's interested in responding, but I could

turn to one of the panellists if you'd like to start. Yeah, go ahead, Reg.

REG LEVY

I have never done a Human Rights Impact Assessment outside of the ICANN situation. I think Farzaneh had walked us through how to do one before. And I think in Prague, you asked me a similar question, and I was like, I don't think of this in terms of Human Rights. I think of this in terms of privacy, which I guess is a Human Right, but that's not how I'm conceptualizing it, right?

Like I have legal obligations to my customers, and I have legal requirements that I have to comply with, and that's what I'm balancing in my head. It tends to comport with Human Rights, because right now I'm bound by laws that support Human Rights, but that isn't necessarily the reason that I'm doing it.

ALAN WOODS

Just building slightly off of what Reg is saying there. I think there was definitely an overlap without a shadow of a doubt, but I think when a data protection Impact Assessment, where, especially when you're thinking of 6-1-F, God, it's been so long since I've said that, and the balancing test that must be taken into account, where it is against the data subjects, data privacy rights is what you need to be balancing. It seems a bit more cursory in the DPIA, or like I have taken into consideration that this is good or bad.

I think the Human Rights Impact Assessment is something that will give more flesh to that aspect, because we were far more focused, I think, for the first 75 billion years of this conversation on, well, the GDPR is scary and makes us have to do these things, and I always think it suffered, that balancing right. Nobody really understood the balancing test. We never really got into that, and I think having that fleshed out.

So, I think there is overlap, but it's like where one ends, the other one takes over, and I think that, and then it all feeds back into the same food.

FARZANEH BADIEI Thank you, and Beth, Beth, no.

BETH MARTY Yes, I did have my hand up, thank you. This is Beth Marty with name.com. I wanted to just highlight, given the really good examples that a lot of the speakers have given about how very nuanced the aspect of registrar discretion needs to be, and how much that needs to be respected for registrars who have to consider a great many things to make a determination, and that given the complexity that's already been shared, how the outcome would probably be rather narrow in terms of what would be allowed to be passed through or disclosed. But I do want to highlight the importance of that, and also the importance of that

consideration for each registrar that is a business that's functioning in a global context. Thank you.

FARZANEH BADIEI: So, actually, I have Mr. Law Enforcement here. And yes, so we made some comments. I think that we should give the floor so that you can make your comments.

UNKNOWN SPEAKER: Yes, thank you. Now I'm from the Hellenic Police here, cybercrime. I want to ask about, for example, Reg, about when you do the balancing test, do you only take into account like if due process is done and completed, or you also take into account the Human Rights of the victims, not only the Human Rights of the data subjects, for example, in child abuse cases where material is hosted online, okay?

Or for example, in phishing sites that are fraud sites that are scamming thousands of people every second, this should be taken into account, like you cannot do an MLAT for a phishing that is ongoing or for so many people are going to lose money, et cetera.

And I want to make a question because sometimes we want to take the data subject private information in order to send a notification of some sort. For example, you've been hacked or whatever. Do you facilitate in any way like the notification of a data subject and if he agrees to put them in touch with a relevant request, et cetera?

REG LEVY

Yeah, thank you for that question. So, it's always a balancing of rights, right? There's the victim, the alleged victim, and the registrant as well. So, when we receive a request for data, we are looking at the whole situation about why they're asking for that data, right? And typically, it tends to be intellectual property concerns. That's just the vast majority of it.

With regard to phishing and fraud that's ongoing, that's DNS Abuse and we will take the domain offline, mitigate the abuse, and then we can have a conversation about whether or not the data should be or needs to be released and to whom because there are security researchers and then there's just like the Italian police who I'm picking up because I've been dealing with them a lot recently.

With regard to CSAM, there's a concept in American law called exigency. If it is so urgent that we can't get a warrant, there are different rules that go into place. So, like if you see me punch someone in the face and then run into a house and you're in pursuit, you don't have to wait to get a warrant just because I'm inside my house now. That's exigent. You know that something has happened right then.

And so, we try to work with law enforcement and have direct conversations with them and that's the key word. Is it exigent? And law enforcement officers know what that means as well and they have obligations so they won't use it unless it is actually an exigent situation. So, there are edge cases obviously and we do our best to

work with law enforcement to support their goals. We do support their goals. I'm not trying to say that I hate law enforcement or want to live in a lawless society. It is just that there are many factors at play and it has to be a balancing test of all of it.

UNKNOWN SPEAKER

Yeah, so what I understand from this is that you only give the data subject information in an exigent circumstance and all the rest of the time you say go through the MLAT channel because I want to comment on it further because we had recently like a year ago a big phishing case that was running in Greece. Like they were making phishing sites, scamming a lot of people, getting a lot of money. And actually, we requested from the registrar the information about the domains.

We didn't get anything. We got it via MLAT. But then again, we did not get any useful information. For example, only the registration information which were bogus. We didn't even get IP addresses that were from the systems that they were logging in that would have helped. And we actually ended up cracking the case just by getting information from Google, from some Google accounts. And like these big companies, I think they are more cooperative with law enforcement in that cases in my experience. And I would like to see that like changing in the future. And yes.

REG LEVY

Right, so I would say that there's no one size fits all answer. I don't just always say, you don't have an MLAT, go to hell. I try to have a conversation about what it is that we're looking for, what I even have. You indicated that you didn't get IP addresses. I don't have IP addresses. But I can help put you in touch with the hosting company because that's probably who my actual customer is and they're going to have the IP addresses.

So, getting you to the right place and getting you the information or the person who has the information that you have to me seems more helpful than just replying with some registrant data. So, I try to solve the problem that is being had as opposed to just throwing around an answer that I think might be the right one.

UNKNOWN SPEAKER

And you don't even have the IP address at the time of registration. I don't keep anything. Okay, another comment I want to make is that following my earlier reply is that these big companies like social media companies, et cetera, they sit on so much more data than registrar seat and yet they are easier to work with.

For example, just a name and an address which may be bogus as we talked before, it's not that private data. For example, you can imagine what Google has so many data and provides apart from content, like, okay, for content, it's different like communication content, but for a notification and basic subscriber information,

they have so many more data and they are easier to work with like they don't put up that many walls. Why?

REG LEVY: So, it sounds like I'm hearing that we don't have data that you want and you can't get the data that we don't have from us. So, go to the people who have the data you need.

FARZANEH BADIEI: Right, so we have a queue here and I would like us to go back to our RDRS. But we have Alan and then Manju.

ALAN WOODS: Thank you very much, Alan, once again for the record. I just wanted to probably thread the needle from what I was talking about back to the RDRS as well. And I think one of the points I may have glossed over and missed was about the order in which when you are dealing with elements of, I suppose, DNS Abuse.

And again, this is coming from my own experience in the deepest, darkest past for myself. We used to get an awful lot of investigatory, very broad, very open requests for data saying there might be something here, we'd like data in order to figure it out. What I'm saying is that in order to properly use data for DNS Abuse, you need to start from that seed, the seed of an evidenced case. Not saying I think there might be something here, it's there is

something here and that makes it a lot stronger for you to make that Impact Assessment.

So, when we're talking about the RDRS, a lot of them are speculative, I think is the word I would think of. And that's what I saw in my experience. We need to move beyond speculation and move into something that is a little bit more concrete in order for us, or I say us, registries and registrars and data controllers to be able to be more readily able to consider and balance and provide data in that instance. So, I just wanted to bring that back.

FARZANEH BADIEI Okay.

UNKNOWN SPEAKER Just one clarification for the thing I mentioned, it's easier to work with some companies. Of course, we go through due process because we always send a prosecutor's order with a request. But I don't know like if you were to receive a prosecutor's order or a court order from another jurisdiction, would you accommodate it? Or you would say to go via other channels like via MLAT or local law enforcement?

REG LEVY So, you can take it, but this is actually a point that I think your point is more about the process that is out there that you can use to reach the registrar and know, kind of like predict what's going to happen, what are the channels of communication and how you can get the

help. It seems like social media platforms have that more clearly documented. Is that right?

UNKNOWN SPEAKER They have established voluntary cooperation channels based on due process and you don't need to go around with MLAT or jurisdiction wise.

REG LEVY Okay. So, it seems like some registrars have that, but I will have you at that conversation offline. But these are very important discussions that we want to actually talk about further. So, but Manju has been in the queue for a long.

MANJU CHEN Not that long, but thank you. I'm happily taking us off this conversation. I just wanted to reflect on a lot of people are saying we should incorporate Human Rights and that assessment in all of our future PDPs and ICANN. And I guess it's our fault that we haven't promoted this enough. But ever since this ongoing PDP, that's now ongoing a lot in their critics, actually Human Rights and that assessment is incorporated in every GNSO working group PDPs. So, it's incorporated in the charter.

Any PDPs nowadays, starting from now, they will have to go through Human Rights and that assessment. None of them have started yet because the PDPs are ongoing, but the staff has been

consulting our experts and NCSGs to understand how to do it. And I think the first ever do it will beat a lot in Diacritics.

And also, for suggestions about incorporating and data protection and that assessment too. That one I think is a great suggestion, but I guess we are not all still kind of confused about what's the difference between that and Human Rights and that assessment. And as the chair of the Standing Committee of Continuous Improvement for GNSO, we are expecting to review the PDP 3. 0 this year or in the coming year very soon. And that one will definitely be taken into account when we review the process. So, thank you for the suggestion.

FARZANEH BADIEI Okay, so I have Michele and Sarah. Very short, like two minutes.

MICHELE NEYLON It's Michele, who's Irish and who's known for his loquaciousness. The ability of me to be brief is limited. Just to a couple of things. First, I think what Reg was talking about in terms of IP addresses, I think that is down to business models. So, it's not that she doesn't have IP addresses, it's the IP addresses she has are not of any use to you because they don't sell direct mostly. They don't sell to the registrant, the end user, they're a wholesale registrar.

Whereas my registrar would have a lot more data that you'd find usable. Now, whether I give it to you or not, it's a whole other conversation, but no, I mean, the thing is, with respect to law

enforcement and MLATs, I understand the frustration. What a lot of us are more than happy to do is to preserve data if you need it.

If you come to us informally and say, hey, this is what the problem we have, this is what we're trying to solve, rather than just going off and getting a warrant or whatever, if you ask us first, can you help us with this? Most of the time, we probably can, or we might be able to say to you, look, that's actually a VPN, and there's no point asking me for the data because I literally do not have it. I never have it, so I can't give you what I don't have. But if you talk to us, some of us have clear policies about which delineate what we have access to or what we can do. So, we're not all terrible, but we're not social media companies.

FARZANEH BADIEI I am sure, I am sure. Sarah, two minutes.

SARAH WYLD Thank you, hi, this is Sarah Wyld. ICANN Org is not my only job, and at Tucows, I have a second part to my role, Tucows. I do data protection impact assessments. That's what I do, it's so much fun, I love it. So, I just want to reflect for a moment on the differences between a DPIA and an HRIA. A Data Protection Impact Assessment focuses on the data and impacts on the data of the processing activity, which could be a Human Rights effect, but I think there are probably more Human Rights than just privacy, I'm not sure, I think.

So, what do I know? I know data, I don't know Human Rights. Yeah, so a data protection Impact Assessment would look at what data is processed and how. How is it collected, where is it stored, when is it deleted? How is the data protected, both technically and operationally? Who has access to the data? And how is the data subject informed of their rights? Those questions are all reviewed.

I don't do a Human Rights Impact Assessment, but I kind of imagine that it would need to start from a set of Human Rights and consider how the processing activity impacts each one. And so, having said all that, I wonder if maybe a Human Rights Impact Assessment cannot meaningfully be done without first conducting a data protection Impact Assessment, as that would inform the HRIA review. And so all that said, if anybody working on the ICANN HRIA process would like to talk to me about the DPIA process, I would be delighted to have that conversation. Thank you.

FARZANEH BADIEI

Wonderful. Very constructive. So, I would like to go back to our RDRS. And I think the first slide that Reg presented is very interesting. Andrea, can we pull up that slide? So, I think Reg mentioned that RDRS form is, she didn't mention this, but this is my interpretation, that the RDRS form is kind of bare bone, and it doesn't provide enough information for the registrar to make an informed decision. Like, for example, it doesn't know who they don't identify themselves. Do they?

REG LEVY: So, the RDRS form basically takes the minimum required data for a WHOIS request and turns it into a form. So question number one is, who are you and what's your affiliation? And so, the form requires name. I don't think it requires, actually, it doesn't require everything, but for the most part, people complete it. What concerns me about turning it into a form is the attestations at the end, where it says, yes, I swear that everything that I have said is in fact correct, and yes, I will treat the data properly.

FARZANEH BADIEI: Okay, great. I can't remember which slide it was. To back. So, we have, yes, exactly. So, we have Sébastien Ducos here, and he's the chair of, would you like to, so Sebastien, do you think that RDRS form could integrate some of these things that the registrars might need?

SÉBASTIEN DUCOS: So, I'm Sebastien Ducos, and I'm indeed the Chair of the RDRS Standing Committee, I've been doing that for the last two years, we're about to finish a two-year pilot, as I'm saying this, I'm trying to read all this, sorry, I have to be honest, I've looked at those forms and in an early stage, it has been a while, I don't see anything that is not in some way or form asked, and the questions are not formulated like that, but it's all in the form as far as I know. Is that your question?

FARZANEH BADIEI Yeah, that was my question. So, it seems like it's kind of like as a basic standard, so the reason I'm asking is that there are some rumors that it is likely for the RDRS, after some kind of gap analysis, to become mandatory for registrars.

SÉBASTIEN DUCOS Can I speak to that?

FARZANEH BADIEI Yeah, maybe.

SÉBASTIEN DUCOS Okay. So, just a little background, two weeks ago, two and a half weeks ago or so, we had a call internal to the RDRS standing committee, we hadn't had calls for a long time, because we were in Public Comments period, and Becky Burr from the Board joined us as the liaison to that standing committee, the Board liaison to that standing committee. And she informed us of a few things that went around very quickly in a spin, and there's a few things that are still a concern to me, but still a few things that we might want to bear down a bit.

The Board has apparently asked staff to produce a gap analysis between what RDRS looks like today, and the policies that are either voted or in flux that could be related to that, and namely everything that has to do with Urgent Requests, LEA

authentication, and PPSAI. They've asked for this gap analysis, we were all a bit surprised because we hadn't heard about it, I also happen to be a GNSO liaison, so I know a bit of what the GNSO is doing, and this is not something the GNSO asked for.

It's called a gap analysis, just to use a different term that is none of our policy agreed term, this is not an issues report or anything like that. And the idea was to see what would be the missing parts between what we have in stock and policy, again at different levels, most of it non-implemented, and what an RDRS would look like. That report is going to be published later this week, the Board has to vote about RDRS because we're running out of the budget, the budget finishes in November, so they have to vote on the continuation of RDRS just to be able to fund it, and at that point part of the vote is also to accept this report and have it published for Public Comment.

I don't know, I haven't seen the report, nobody's seen the report, maybe the Board members have, but I haven't, and so it's a discovery for everybody, and I strongly encourage everybody to read it and participate in that Public Comment.

One of the things that transpired from what Becky Burr was saying was that mandatory participation of registrars, not of requesters, as you said, Michele, but of registrars is being contemplated, in the sense that it's no use to have a centralized system if not everybody participates in it.

I personally would like to open the conversation, and we've had that conversation already in RDRS, where if, and I'm going to take Reg's example, and I hope you allow me, but if you are an operator that has a system that is equivalent or better than RDRS, that has everything automated and in place, RDRS should invite users that need to communicate with you to use that in the easiest possible way, with a link directly to your site, they don't have to read 20 pages of instructions and figure out what they need to do, they need to be directed there, but then that would supplement your participating in RDRS, because you're still part of that centralized system.

I'd like to propose that. We proposed that, and there was a recommendation towards that, let's see. We need to be a bit careful here, definitely, because for once, my limited experience in once I see the Board indeed started to shuffle a few things of policy and bringing together things that maybe, as Michele said, maybe it's not their position, it's not part of the bottom up when the top decides.

They're very, very clear in saying we haven't made any decision, the only thing that we're trying to do is to shine a light on what we have, what the landscape looks like and what we're missing, and then we'll have to communicate on it. So, let's not all immediately get on our horses and read the document, but at the same time, let's do read the document. It's coming, it's being published, it will be published at the end of this week. They're voting on Thursday and it will be published immediately after. Yeah, absolutely, I agree

with you. Why do we need to know about a document that is going to be published and they're taking seemingly decisions on it? I don't know. But let's see it coming.

Do participate in the Public Comment. It probably will run until the end of the year or mid-January, something like that. It's not the best convenient time for these things, but keep an eye on it because there will be things in there. There's many, many things that can be said about it, but we need to read the document before we start getting too antsy about it.

FARZANEH BADIEI Okay, so I'm just going to make this comment and then we go to Thomas. If this becomes mandatory, then law enforcement authentication has to happen before any law enforcement makes requests through that system.

SÉBASTIEN DUCOS Sorry, I didn't make it clear. The gap analysis is not going to say this needs to be mandatory. The gap analysis is going to say something like, hey, if we want a centralized system, it makes sense for people to participate. Go and build, go and negotiate, go and discuss policy that makes sense in that perspective. If we're building something central, it needs to be used by. They're not saying we're going to make it mandatory from tomorrow. They're not saying anything. They're going to say, here is a gap in policy that we need to fill. If we mean this to be central, we would assume that

participation, which is basically the wording, by the way, of what SSAD was. It's about as clear and as clear.

FARZANEH BADIEI: But SSAD had accreditation. There were other accountability mechanisms which can hamper Human Rights. We cannot just jump into this. It's just not acceptable. Go ahead, Tom.

THOMAS RICKERT: Thanks so much, Farzi. In terms of potentially constructive way forward and how to deal with this in the months and years to come, I mean, the DPIA for the RDRS should have been conducted by ICANN or whoever is running it before it was launched, because that's an exercise that you typically do before you start new processing activities to check whether there are risks that are acceptable that can be mitigated and all that.

So, the Human Rights Impact Assessment is an additional layer. So that's beyond the data that's potentially being passed through the RDRS or disclosed to third parties, because a wrongful disclosure can lead to discrimination of the data subject concerned. It can lead to impairing the right of assembly.

So those would be the additional factors. And Farzi, you and your group have negligently built a reputation for doing Human Rights impact assessments. So, why not proceed with it, even with some assumptions? What does the RDRS do on Human Rights as it stands

in the pilot? What would change if it were mandatory? What would change if we had an accreditation system in place?

And then give that as a solid basis for the community to take into consideration when discussing this further. I think in a perfect world, you could probably manage all the risks, but we need to make sure that at least we know about the risks that could occur and what points to cover in policies and technically to make sure that the risks are mitigated as much as possible. Does that make sense for you?

FARZANEH BADIEI Yes, yes. Thank you. That was the purpose of this. Yes, for sure.

THOMAS RICKERT But I don't think that RDRS has anything to do with Human Rights. The balancing test that follows has to do with Human Rights. The RDRS is just a mechanism that puts us in touch with the register.

FARZANEH BADIEI That would have been fine if it was not mandatory to opt in. And I understand it's a triage system, but I did lay out in the beginning, if it becomes mandatory, it could have an effect on the registrar's incentives. They might not do that, a fundamental rights balancing. And I have discussed this, we have discussed this with the Board. We cannot contractually make the registrars to do

fundamental rights balancing. At the moment, we don't have those mechanisms in place. So, and I don't know if I can--

I'm going to make my registrar friends very unhappy. We might have to push for mandatory fundamental rights Impact Assessment in your contracts. But that's not going to happen because they said that's like the picket line. Anyway, but yeah, go ahead.

THOMAS RICKERT A quick two-finger on your point. And I think we should continue this conversation somewhere else. You said the RDRS doesn't have any impact on Human Rights. I think the point that Reg made earlier is we should remember. Namely, that at the moment, the system is designed so that folks just tick every box, I've done everything all good, submit the request. So, that's a design point, so you can make sure that during the submission, certain information is input to make sure that the requestors have actually done their due diligence before submitting a request.

And those are the points that I think can be covered in a Human Rights Impact Assessment that anticipates different variations of the RDRS so that it can be taken into consideration when designing or not designing certain things.

FARZANEH BADIEI That's a very good point. And I think that's what we can follow up on. Reg, famous last name.

REG LEVY

So, I wanted to speak to the mandatoriness and the voluntariness and all that. Tucows participated in the RDRS pilot because we wanted to gather the data about who was interested in using it and how much it would actually cost. And the RDRS has done that. And at the point that that was done, we withdrew our voluntary participation for the very reason that it should not be mandatory in the current form. And because we were getting better results from having people do it manually and not operationalizing the check, just check all the boxes. Yes, check all the boxes.

We had people requesting, claiming that they were law enforcement because that escalated their requests. And they were not law enforcement. So, like, all kinds of issues that presented specifically because the minimum required information for who is data request was turned from a list of questions into an online form, that that's where the issue began. And so, returning to that has given us a far better dataset of successful requests. And by successful requests, I mean, people got the data they wanted. And so, they were going through RDRS.

We weren't getting what we needed. And we switched back to what we had been doing before. And everything improved. So, I don't understand how the data that RDRS gathered proves that it should continue.

FARZANEH BADIEI	Great. With that, we are at the end of this session. Thank you very much, everybody, for attending. We have work to do. And we will be in touch. And this is going to be a series of Human Rights Impact Assessment sessions. And the focus, I think, in the near future is going to be RDRS. Thank you.
ANDREA GLANDON	Thank you. You can stop the recording.

[END OF TRANSCRIPTION]