ICANN86 Seville | PF – GNSO: ISPCP Outreach Session
Wednesday, June 10, 2026 – 16:30 to 18:00 CEST

DEVAN REED

Hello, and welcome to the ISPCP Outreach session. Please note this session is being recorded and is governed by the ICANN Expected Standards of Behavior, the ICANN Community Anti-Harassment Policy, and the ICANN Community Participant Code of Conduct Concerning Statements of Interest. Please observe the following guidelines when participating in this session. I will also post them in the chat for your reference. Only questions posted in the Zoom chat identified as a question will be read aloud during the session, as time permits, when directed by the chair of the session. If you wish to speak, please raise your hand in Zoom or otherwise as directed. When speaking, please state your name for the record and speak clearly at a moderate pace. I will now hand the floor over to ISPCP Chair, Philippe Fouquart.

PHILIPPE FOUQUART

Thank you, Devan, and good afternoon, everyone. Welcome to this ISPCP Outreach session. Welcome to those who are in the room and to our remote participants. As it happens, we have more participants remotely than on-site, which is, I don't know if it's a good thing or a bad thing, but anyway, there we are. This is the fifth edition of our collaborative effort with OCTO and SSAC. We've had

three webinars. For those of you who may be interested, please have a look at ispcp.info. That's our website. Shameless plug: for those of you who work for an ISP and with whom we wouldn't be in touch, please have a look. I think Lars will say a word about how you can join our constituency, and we'll be in touch. With this, I'll let Lars elaborate on how we will proceed. Lars?

LARS STEFFEN

Thank you very much, Philippe. So good afternoon, and good morning, and good evening for those who are participating online, so wherever you are. Welcome to today's ISPCP Outreach session on Data Sharing for Abuse Mitigation: Balancing Privacy and Security. My name is Lars. I'm the vice chair of the ISPCP, and if you meet me in a different context, I'm also the Head of Infrastructure and Resilience at eco, the Association of the Internet Industry, and also the Vice President of EuroISPA, the European Association of National ISP Associations. As Philippe just mentioned, this is a part of our series of outreach activities throughout the year. We do monthly webinars on different topics, so the most recent one was on DNS blocking. And we do on-site sessions like this at every ICANN meeting. After the summer break, starting in September, we will continue with our webinar series in close collaboration with SSAC this year, because what we learned last year through our last series of webinars and outreach activities is that DNS abuse and security-related matters are currently of high interest, and this is what we would like to serve. If you're interested in participating and joining the ISPCP, as Philippe also just mentioned, please visit

our website, ispcp.info, where you can also find the online form to apply for membership. Eligibility criteria: you're an ISP or an access provider or an internet exchange point, or you provide internet access to end customers and end users, or you are a trade association representing those entities.

Today, we would like to shed some light on abuse. Online abuse continues to evolve rapidly, and criminal actors are becoming more sophisticated. Attacks are increasingly automated, and as we've already learned this week on Monday, they are also increasingly AI-supported. And effective mitigation often depends on timely access to actionable information. At the same time, data sharing must be handled responsibly with due process regarding privacy, data protection, legal obligations, and of course, also the rights affected by individuals. And this session is intended to explore that balance. How can operators, public authorities, and also researchers and other actors share the data needed to prevent or mitigate abuse while ensuring that privacy and security are both properly protected? And where is fast action required? Where is more careful assessment needed? And how can we avoid treating very different types of data and risk as if they were the same? So we will shed some light on the different data elements involved in this process, also from an ISP perspective, which go beyond registration data for domain names. And we will begin with an introductory presentation by Thomas Rickert on my left and, from your perspective, on the right of this table. He's the Director of Names and Numbers at the eco Association that I work for and

Managing Director of his own law firm, who will frame the issue on operational, legal, and policy perspectives, looking at the types of data involved, the actors in the ecosystem, the different risk levels, and possible legal bases for responsible data sharing. And after that, I will hand over to Tara Whalen from the SSAC. She will be joined by Gautam Akiwate, also from the SSAC, and Sarah Wyld from the Registrar Stakeholder Group. And together, they will bring operational, research, and compliance perspectives to the central question of the discussion: how can operators share actionable data to combat online abuse without overstepping privacy and data protection laws? And with this, I would like to hand over to Thomas.

THOMAS RICKERT Thank you so much, Lars, and welcome, everyone. This is the part of the ICANN meeting that you've all been waiting for, so it doesn't get any better than that. This excellent panel. The topic is great. Just the air conditioning is so loud that I hear that louder than Lars speaking. I hope that the audio is okay for you. So we're going to talk a little bit about data sharing for abuse mitigation, and the topic is balancing privacy and security.

Now, what we have in store for you today is to talk about the following topics. I will just spend a few seconds talking about who eco is and what we are doing there. Then we're going to talk about the issue at hand. What's the issue that we're trying to solve with data sharing? I think we also need to be precise as to what we mean

by data. So what data are we actually talking about when it comes to data sharing? What actors are involved in the data sharing? We're talking about threats and the associated risks, security, and legal considerations. And now this looks like we're talking about legal points the least, but actually that's going to be the bigger part of what I'm going to discuss. As Lars mentioned, eco is an association that has different types of intermediaries among its members. So it's more than 1,000 members from more than 60 countries. And our members have asked Lars and myself in particular to shed some light on what areas of collaboration we can utilize more than previously so that we can become better in abuse mitigation across sectors. Because at the moment, we're still seeing a pretty siloed approach where registries are doing something among registries, the registrars are talking to each other, but hosting companies talking to domain name players, CDNs, payment gateway providers, and others, that's the challenge that we have. And with the topDNS Initiative, we're trying to tear down these silos a little bit.

Now, the issue is that we need to get faster. We're seeing that the criminal landscape is getting increasingly sophisticated. This is no news to you, but with the advent of AI-supported attacks, the challenges become more complex, and the industry really needs to up its game. Then, we also know that we need to get mitigative action in matters of minutes rather than hours or days. And if you look at the way wholesale companies are talking to their resellers or reseller chains at the moment, the system doesn't seem to be

fast enough to be able to help with the challenges that we're facing. So emergency cases need fast responses. And at the same time, if we have taken mitigative action in emergency cases, the investigations associated with that can potentially take longer. So we need to take a look at what are we trying to achieve and adjust the service level or the response times according to that. And what we are seeing in our discussions is that sometimes companies just talk about data sharing as one block, if you wish. But we need to take a look at it in a more nuanced fashion. And I'm going to try to set the scene for that a little bit today.

So what are we trying to achieve with data sharing? Is our primary interest disruption? Do we want to suspend websites? Do we want to suspend domain names or do takedowns? Are we interested in attribution? Do we want to find out who is behind an attack, what state actor might be behind an attack? Or are we interested in holding individuals behind criminal activity to account? Because I guess that's one of the major issues that we're facing these days, that there is so little deterrent that criminal action is still a worthwhile exercise, with almost no risk for the individuals involved. Are we interested in prevention? Do we need the data in order to prevent harm from networks or individuals? Or are we interested in strategic planning? So some folks, including the European Commission, are interested in getting transparency reports from service providers so that they can allocate resources. They know what threats are emerging, and how do we need to

allocate resources and funds to activity that governments or private actors need to take?

All right. What data are we talking about? I guess the biggest distinction that we need to make, and this is going to become very relevant during my talk and I trust also during the subsequent intervention, is that we need to make a distinction between personal data and data that is not personal data, because personal data enjoys special protection, whilst data that is not personal can, in most cases, be shared pretty freely, unless it's, let's say, trade secrets that are involved. In the domain name industry, that's primarily the domain name itself and public registration data, and then we have non-public registration data. We have account holder data, and it's sort of interesting that we are, in our policies, primarily talking about registration data, i.e., what data is associated with the domain name registration, whilst the payment data, follow the money, and other data is sitting with the account holder. And our policies don't really speak to that. Then, since this is the ISPCP Outreach session, let's talk about other actors beyond the domain industry. And a prime example of that being covered is the upcoming e-Evidence regulation that's going to kick in on August 18th this year for players that are offering their service in the EU or to the EU. And there we have a distinction in the law between subscriber data, data for the sole purpose of identifying a user, that can be an IP address if it's dynamic with a timestamp, for example. That can be traffic data or content data. And then I think in our discussion, we also need to make a distinction between

information and threat intelligence, because not everything that's information is helpful in our work against abuse. But the data that individuals might have and that might seem almost useless to them might be able to be enriched by others and then become threat intelligence upon which other actors can take action.

So trade secrets, I already mentioned. That's going to play no further role in this discussion today, but you need to be cognizant of the fact that not all information, even if you want to share it, can be shared, even if it's non-personal data, because it might enjoy special protection as a trade secret. And let's not forget, in many cases, the data that's involved in abuse is either evidence of abuse that happened in the past or ongoing abuse. And that is particularly relevant when it comes to things such as CSAM. So we also need to be cognizant of the victims involved, because one of the big issues for victims of sexual crimes is the secondary traumatization of them knowing that the data, pictures of them, are still being circulated. So we should be very cautious with the information that we might have on our systems relating to that.

Okay, the actors. In the ICANN world, we have ICANN, registries, registrars, resellers, privacy and proxy services, and other service providers. Then we have the regional internet registries that allocate IP addresses that also have data that's important when it comes to fighting crime. Then we have hosting companies, and in that regard, it's important to make a distinction between managed and unmanaged hosting because they can't take the same level of action. We have access providers, telcos, email service providers,

payment providers, and others, and together, I would call them service providers. And they are primarily the ones that are on the disclosing end of things. Some of them are receiving information as well, but the primary customer group, if you wish, for asking for data are law enforcement authorities and other governmental authorities, researchers, rights holders, and others that have claims they want to raise where they need the information that's not publicly available. We have threat intelligence providers, CERTs and CSIRTs, and others.

Now, what threats are we actually talking about? I guess the primary concern is the well-being of victims of illegal activity, folks that have been defrauded or otherwise fallen prey to illegal activity. Then we have the risk to critical infrastructure. We have the risk of becoming a victim of illegal activity. That's where the preventative side of things comes into play. We have the risk for data subjects, whose data might unlawfully be disclosed so that they might be at the risk of being harmed later. Then we have the risk for the service providers involved, because if they unlawfully disclose, they themselves might face risks, with claims or sanctions or penalties being raised against them. And all these have different risk levels, and we should always take a risk-based approach in determining who can do what in this game. So my graphic skills go as far as it gets on this slide, so I've put in an arrow for your benefit. So potentially the least risk is involved with non-personal data, unless, let's say, it's involving trade secrets. Then we have the processing of personal data, for example, in associated domain

checks. That's the PDP number one that we're currently working on. So the risk of performing these ADCs is pretty low. So doing that in itself is not really an issue. But if you, as a response, start changing name server entries or suspending domain names, putting them on a lock or something, that's where the risk for the individuals or the parties involved is getting bigger. Then we have the risk of unlawfully disclosing registration or subscriber data, the risk of disclosure of traffic data, and then potentially the highest risk is involved in the unlawful disclosure of content data.

Now, when it comes to security, and I guess this is no news to you, being part of the infrastructure service providers, is that we always need to be concerned about the integrity, availability, and confidentiality of data. So even if you share data, you need to make sure that the data that you share is accurate, that it's not being tampered with, that you potentially sign the data that you're sharing so that it can be checked for accuracy. Only today, in my legal practice, I had a case where a service provider disclosed data to a law enforcement authority, and the law enforcement officer, or the prosecutor in that case, got back to us and said, "Well, the table that you sent seems to have an issue with it. The data fields don't really match." And then if you don't take proper care of that, that might lead to you being the cause of somebody being a suspect in a case that shouldn't be. Right? So we need to be careful that the data that we're sharing is not compromised. And in order to achieve that, we need to have proper policies in place, but also

proper technical and organizational measures to make sure that the data is always accurate.

Now to the legal considerations. You always, at least in the jurisdiction that I come from, which is European, need a legal basis for processing personal data. And the legal bases that come into play when it comes to sharing data to mitigate abuse are consent, although it's pretty unlikely that you will obtain the consent of a data subject whose data is involved in criminal activity. Then you might need to process data to fulfill a legal obligation. Let's say there's a statutory duty to disclose data to law enforcement, then you can disclose that data without needing an extra justification for that data processing, or share the data based on a legitimate interest. And that is where a balancing test comes into play. So you need to weigh the interests of the data subject concerned, let's say the holder of a domain name or the person behind an IP address, and weigh that against the risk involved for the party concerned or the benefits that others might enjoy if you, for example, prevent them from being defrauded. And then if you are talking about globally sharing data, you also need to think about international data transfer safeguards to make sure that you only disclose data that might put folks at harm to a jurisdiction that has appropriate legal safeguards in place.

All right. It goes on. General rule is, if no personal data is involved, just share the data. That shouldn't be an issue. If you are concerned about email addresses, IP addresses, or otherwise of spammers or wrongdoers, we've done a legal assessment on that a couple of

years back, and our conclusion was that those who are freely sharing their own data with sort of an unlimited number of recipients have relinquished their rights into that data. And also the question is, how big is the risk that a spammer will ever go after you because you shared their data? Because then they will be forced to step out of the darkness and show who they are. So the risks for you are pretty low.

So if you're sharing data to a law enforcement authority or other public authority, if you are talking about a domestic law enforcement authority, that's pretty much always covered by applicable law, so you do your due diligence and then you disclose. If you are asked to disclose data to non-domestic law enforcement authorities, things become a little more tricky. So if there is a mutual legal assistance treaty in place, then you can go through your local authority and share the data through that official channel with the authority in the requesting country. But if there's no such mechanism in place, you can still share the data. So you can share data with basically every country in the world, and law enforcement as well, if you have done a case-by-case legal analysis that led to the risk of disclosure being acceptable. Right? The fact that there's no MLAT or other legal mechanism in place does not mean you can't disclose. You just need to be more diligent and apply the proper legal checks. If you want more details on that, check out the guidance by the European Data Protection Board. It's guidance 2/2024 that basically says you need to be cautious, but you can disclose if the parameters are right. But then we see a new

era starting shortly. That's number one: under the e-Evidence regulation and the associated directive, law enforcement from other countries can ask for data directly with the service provider. So it's no longer the relationship between you and your domestic law enforcement, but you disclose directly to non-domestic law enforcement authorities. Right? And in e-Evidence, that is happening through an official IT system that they're currently finalizing, and that is also applicable to service providers that are offering their services to the EU. So even if you're not established in the EU, you may need to find a legal representative in the EU and then disclose the data based on orders that are addressed to your legal representative. But that would basically give you the legal certainty that you can disclose even cross-border. And then we have the second additional protocol to the Budapest or Cybercrime Convention that also foresees the disclosure requests being handled internationally for, let's say, non-public registration data for domain names. The second additional protocol is not yet through the process of being ratified, but it's in the making, so you also need to keep that in mind as a legal instrument for global data sharing.

Okay, the next scenario, we've now discussed service provider to law enforcement, is service provider to rights holder. So you have, let's say, an IP lawyer or a company that has been hacked that says, "Okay, our intellectual property has been compromised. Trade secrets have been exfiltrated from our network. We need to know who's behind a certain attack." Then you may even have a

statutory obligation to disclose that data even to a private entity. But most cases, I guess, will need to be handled based on a legitimate interest. So if the parameters are right, if the situation is right, you may be able to disclose that data, including subscriber data or non-public registration data, to claimants of intellectual property rights. Then service provider to researcher. I know that one of the subsequent speakers is going to talk about researchers, but you need to check in the laws that are applicable to you whether there are special derogations for researchers. In Germany, for example, we have a derogation for research data for medical purposes where you can, if the balancing test is okay, disclose even health-related data to researchers if the interest in the research is outweighing the risk of the patient in that case. And then service provider to service provider or service provider to threat intelligence provider, I think we can say, check out what data elements are actually concerned. One of the protocols that are being used to exchange threat intelligence is X-ARF, but most of the data elements in X-ARF are not personal data. So you have the domain name in it, you may have an IP address in it, maybe a URL in it. That can be personal data, but it doesn't necessarily have to be personal data. So I think you can be pretty liberal in sharing that because the domain names are populated through the DNS anyway. IP addresses are not that big of an issue, and actually in the EU, there's currently a discussion of diluting the definition of an IP address as personal data. So those are the only two data elements that we are discussing in this context.

So again, the question is, what are we interested in achieving? Are we interested in disruption and takedowns? So in that case, IP addresses, domain names, are the primary source of personal data. And I think in many cases, if not in all cases, the balancing test will grant you the right to share that data. So if you find something in the domains under management that you have, a phishing campaign, let's say, where domain names are involved, and if only the registrar or a neighboring registrar knew that domain names are involved in a phishing campaign, and if the registrar could take that down, that could prevent innocent users from being defrauded. So bear that in mind. It becomes more challenging when it comes to attribution and prosecution because that's where you share more than the IP address and the domain name or URL, and that is to be handled with more care. But again, there might be a legitimate interest that you can claim to disclose that data, or you might even be forced to disclose the data to fulfill a legal obligation. Are we interested in prevention? Again, in these cases, it's primarily the IP address and the domain name that are in question. And are we interested in strategic planning? Think about using aggregate data so that you don't need to specify individual data sets, or think about anonymization or pseudonymization of those data elements. That can help authorities and others that want to allocate resources to fighting abuse in a position to work with that data as well.

So my last slide for today is, what am I asking you to do? Work with threat intelligence providers. If a registry or a registrar, it really

makes a difference whether you are only reacting to abuse reports that you are receiving from the outside or whether you are using someone who can help check whether the domain names that you have under management are no issue or whether you have issues. And if you have that information, then you may be able to take action before abuse hits your abuse desk, and that might help you save human resources and ultimately costs. So be proactive, try to be ahead of the curve. Share intelligence with other providers. Even if you think that what you have to offer doesn't help, if it is aggregated and enriched with data that others have, your information becomes intelligence, and that can really help make a difference. Act swiftly. Try to be as fast as you can in sharing the data if you can. If you have resellers, and that applies not only to registries and registrars but also to hosting companies and others, try to have proper contracts and acceptable use policies in place. We still read a lot of reseller agreements where the general rule is that you give a reseller 48 hours to respond to a report. Right? And that is, in most cases, not fast enough to live up to the challenges that we are facing today. Sometimes when we're talking to companies, they say, "Yeah, we do engage in data sharing." But for them, data sharing is a one-way street, so they only want to receive data. But specifically when they're talking to their legal departments, they say, "Don't share." Right? And that, I think, is something that we need to change. It is a two-way street. You need to make sure that you pave the way for being able to share intelligence and information that you have inside the organization to the extent that you have the legal possibilities and that you don't

violate trade secrets, for example. And lastly, be bold. I think you can't protect yourselves against each and every risk there is. I could be hit by a stone falling from the roof once I step out of this room. Right? So there's no free ride. But I think if we want to make this ecosystem a better place, we need to take some risks, and as long as the risks are manageable, I think we should go for it. That's it. That's all for me, Lars.

LARS STEFFEN

Okay. Thank you very much, Thomas. That was already a lot of information. So do we have any questions on this? Do we have questions in the room or do we have questions online? Also, just to give people the opportunity to take a breath. There is one hand from Anil.

ANIL KUMAR JAIN

Thank you, Lars, and thank you, Thomas, for a wonderful presentation. The basic objective of these discussions is to protect the end user, that there should not be any harm, whether it is a commercial harm or non-commercial harm. Now, here, when we are talking about the actors involved, I'm just wondering, once the actors involved share the data to the concerned authority, whether it is LEAs, domestic, international, or anybody, what protection these actors have after we share the data? It means that once we share the data, then there are some processes, and we found outcome has come. Some people have been caught, but at the

same time, those actors who have provided the data, they have to be safe, that they should not be harmed in future. Thank you.

THOMAS RICKERT

Thank you so much, Anil, for your kind words. I have to admit that I had a hard time discerning what you were saying because the audio in this room is challenging. I heard the question on what safeguards can we put in place in terms of what happens with the data once we disclose it. And I would recommend that if you not only anecdotally share data, but if you enter into a continuous data sharing with third party, that you put data sharing agreements in place where you request the recipient of the data to apply purpose limitation to the processing of data, i.e., that they must not use the data for other purposes than, let's say, research or abuse mitigation, and where you also specify the parameters under which the data may be disclosed to a third party.

LARS STEFFEN

Thank you very much, Thomas. There is another question in the chat from Kurt Jaeger about firewall reject logs, but Sarah's already in the process of responding to this, that it depends on which data elements are exactly included in those logs. Besides this, I don't see any other hands, and I think that would be now the right moment. Oh, I'm sorry.

AERYN VAN DAELE: Apologies. Aeryn, for the record. Is there any consideration to assessing and flagging potentially spoofed or otherwise falsified provided data? Or worded differently, how do we make sure that a malicious actor cannot simply use previously acquired personally identifying information from others to register a domain, for example, and thus have the already victimized person put into trouble with law enforcement, for example? Is there any consideration towards that?

THOMAS RICKERT: Shall we open it up to the entire panel? Maybe Sarah, this is something that you also want to talk about?

SARAH WYLD: Hi, this is Sarah from the Registrar Stakeholder Group, but I think right now I'm representing Tucows, not the stakeholder group. That is a great question because that is a real problem. Sometimes people put wrong data on domain names. There are policies in place that require people to provide accurate data. If we are informed or aware that the data is wrong, then we require the person to update it, and there are processes to verify that. But it is definitely a thing that happens, and that needs to be watched out for and protected against.

LARS STEFFEN: Thank you very much. So shall we take the opportunity? Tara, I would like to hand over to you.

TARA WHALEN

Thank you, Lars. So welcome to the panel portion, which maybe you've gotten an early look at thanks to the participation we're already seeing on the panel. So I'm going to, if we have the slides up for that session. Sure. I think we have a panelist bio slide before that, but I am pleased to be joined. There we are. Look at my panelists.

I want to give a moment to introduce them properly because they have a range of expertise, knowledge, perspectives that will inform the conversation today. So I am joined by Gautam Akiwate from the Security and Stability Advisory Committee. And so Gautam is a researcher, and his research lies at the intersection of security and networking, using empirical methods to study the complex ecosystems that make up the Internet. He is particularly interested in understanding the form and function of core Internet infrastructure and how attackers undermine the security and stability of the Internet. And his work has received multiple awards at top networking and security conferences, including three IETF Applied Networking Research Prizes. So he brings that to the table, and we're glad that you joined us today.

And I'm also joined by Sarah Wyld. She is, to get this correct, the Vice Chair for Policy of the Registrar Stakeholder Group. And she is also the Head of Policy and Privacy at Tucows, a domain name wholesale registrar and registry operator, a fiber ISP, Ting, and mobile services enabler, Wavelo, where she helps make the

Internet better by championing the privacy of Tucows's customers and employees. Sarah leads Tucows's privacy and data governance program, including creating data processing policies, drafting staff training modules, and implementing solutions for compliance with global privacy and data protection laws. So you can definitely see very relevant expertise for this discussion. And I am delighted to moderate a discussion with these two experts whose interests overlap so much with my own. So I'm Tara Whalen, and I'm here with my SSAC Vice Chair hat on. But also I am Principal Privacy Specialist at the World Wide Web Consortium, W3C. I previously worked in technical privacy roles in industry, including at Cloudflare, Google, and Apple. And I also worked at a regulator, the Office of the Privacy Commissioner of Canada. So I have a PhD in computer science and a Master of Laws with a concentration in law and technology. And to my perpetual surprise, I have spent over 25 years in the information security and privacy fields. To the next slide, please.

So we have a core question to tether our discussion today, which was: how can operators share actionable data to combat online abuse without overstepping privacy and data protection laws? So of course, as a privacy advocate, I always like to say that the legal requirements are sort of the floor or the foundation for your privacy obligations. But I really hope that organizations go further where they can to advance privacy. But it's of course vital to ensure compliance. And so I've highlighted on this slide a few of the topics that we expect to cover today, which we identified during our

planning. But we did design this session to be very conversational, and I'm looking forward to a lively interactive discussion. I know that we're competing with another AC, which is the HVAC, which has entered the room and is making it a little difficult to hear. So we'll do our best to work around that, and we will take questions from the audience and work those into the discussion. So with that, I'm going to start off with Sarah really to speak to that core question. You see things from an operational perspective. You have this deep privacy expertise. So how would you begin to address this trade-off?

SARAH WYLD

I know. I told you not to move the mic, and then I just did it. Okay. As a domain name registrar, which I think is included in the category of operators, we are a data controller. So we can share registration data that is personal data with third parties who demonstrate a legitimate purpose to access that data. And one legitimate purpose could be combating security risks or DNS abuse, which are often similar, not exactly the same. So with that in mind, in terms of requests for registration data disclosure, I thought it might be interesting to share some data about the volume of security requests that my registrar has received. And I will just note that we've talked about phishing here and DNS abuse, which is often reported to us, not as a security issue, but as a commercial litigation issue. Someone's dealing with their trademark. But here, because I was asked to be here by the SSAC, I've really focused on the security requests that we receive. So

before I forget, I'm just going to link in the Zoom chat. There you go.

Okay. So Tucows has been tracking disclosure request and response rates since 2018, so about eight years already. And we've documented just under 7,000 requests in that time. Of those requests, can people guess how many came from security practitioners? Seriously, just anybody take a guess. Out of 7,000 requests, how many were for security? Hand up in the Zoom, just type it in. I want somebody to make a guess before I say it.

LAUREN THOMAS I don't imagine that many.

SARAH WYLD Pick a number. How many do you think it was?

LAUREN THOMAS Maybe 3 or 4%?

SARAH WYLD Okay. Thank you. And then I see in the Zoom chat, I've got 6,500, 40%, less than 10%, and 5%. So I will tell you, it is 86 requests. That is 1.3%. Okay. So that's one thing. Another thing that we track is the rate of abandoned requests. Now sometimes, a disclosure request doesn't have enough information for us to make a proper decision. Usually, it's missing context about why they want the data. My favorite part is when they don't tell us what domain name they're

interested in. Yes. So that happens, and so for the security requests that we've received, 25% of those 86 requests were incomplete, and they didn't respond to our request for more information. So bringing it back to the question, operators can share actionable data when that can be done in a legal context that permits that sharing. And so for registration data, that means giving us a well-formed and actionable request that explains why the data is needed and hopefully is clear about how getting that data relates to achieving the security goal. And if you want more specifics on those numbers, they are in that link that I just posted. Thank you very much.

TARA WHALEN So if you can speculate, why do you think that the number is only as low as the 86 that you received?

SARAH WYLD Thank you. So we think that the previously public WHOIS data, while it was useful before 2018 when it was publicly available for everyone, seems to not actually have been the source of the most relevant data for addressing DNS abuse or apparently security issues. And since the data became redacted, we've not seen a notable decrease in DNS abuse reports, in security reports that come through that side, which tells us that the lack of WHOIS data does not mean that these issues cannot be identified and reported.

So we've heard some complaints about it, but those aren't coming from the people who are actually asking for the data.

TARA WHALEN: And I think I'm going to rope in our researcher. Oh, we have a question. We have a question from the floor. We'll take that.

LAUREN THOMAS: Hi, Lauren Thomas, for the record. It's not so much a comment, but sharing some of my experience working in security. Since WHOIS has been essentially sunsetted, I've found that people I've worked with know that RDAP exists, but they don't really understand how they can get access to the tiered information unless it is a consultancy company that specifically does security research. I know I've had things where we've had phishing emails come in, and I try and identify who's behind the domain. And previously with WHOIS, that was really easy to do, and genuinely I do think RDAP is a better solution. Don't get me wrong, I really do. But we're not immediately reaching for it now because we know the chances are it's either behind the privacy shield or the data just isn't there. And so maybe just increased communication with people who work in security more generally, and not just security researchers, is possibly necessary.

SARAH WYLD: That is a very good point. Thank you. I agree with increased communication.

TARA WHALEN

Thank you. And I know we have a researcher at the table who may have a perspective on this as well.

GAUTAM AKIWATE

Yeah. So as a person who does empirical measurements, one of the things that we tend to like is large amounts of data, and some of the openness data efforts like CZDS have really helped us. RDAP has helped us. And what we find is getting information from whatever is out there is super helpful. And more or less, as a researcher, not as a security expert or a person who's working in the industry there, but as a security researcher, we're interested in broad trends as an academic. And what we're not interested in is specific details of a specific registrant. What we would rather like to know is, is this the same registrant behind the domain? And I think that gets to some of the privacy aspects where I would rather not know what's the registrant's address or telephone number, but I would rather want to know, is it the same registrant behind all of these domains? And I feel like as a researcher, I'm always in the "what is possible" land as opposed to "what is there now," and I think this is one of those improvements that we could do as we are sort of thinking about what should exist. And so as I was going to say, one of the things, I was going to push back against the balancing security and privacy aspect, because balancing security and privacy sort of implies that privacy comes at the cost of security, and that's a spicy take.

SARAH WYLD Yeah.

GAUTAM AKIWATE Pretty spicy take, but I figured it's Wednesday and we don't have a lot of people here, so nobody's going to find me. But the argument there is that I feel we do a disservice to folks when we sort of conflate privacy and security, and say privacy comes at the cost of security. And a quintessential example that comes to mind is encrypted DNS, where at ICANN, everywhere you go, people are like, "Oh, how do you defeat DNS blocking? It's DNS over HTTPS." And that's objectively not true. If you look at things that are happening in Italy, in France, that is not at all true. And we have some colleagues here who have worked on research that look at Piracy Shield, and they are basically forcing DNS over HTTPS operators to do the same. So my point being, it's not related to abuse, but we shouldn't look at this as a balancing act. Rather, there are things that we can do on the privacy front while still getting the same security benefits. And that example being in the RDAP information, I don't think I need the registrant information. Rather, an identifier saying, "Hey, this is registrant number five," and I'm good with that. I just need to know whether it's the same registrant or not. I don't care about the telephone number, as I said before.

TARA WHALEN If I can get you a little more, because I appreciate your perspective on the use of data and writing papers, and I spent a bit of time in the research space as well, and there can sometimes be a gulf between theory and practice. And I don't know if you can talk a little bit about the value, sort of in general, of being able to use the real-world data when you're writing an actual peer-reviewed research report.

GAUTAM AKIWATE So using real-world data is great because then you can uncover real-world problems. And some of the research that we did uncovered real-world problems with operational practices that happen at some registrars. And they're typically of the form, like the protocol did not specify the limits, or there are some corner cases. People made educated guesses as to what it should be. Sometimes those guesses turn out to be wrong, and thereby, they created a security risk. And I think security through obscurity is not great. And I feel that there is a tendency, and I'm sorry, I'm going for a lot of hot takes today, but I apologize.

TARA WHALEN Yeah.

GAUTAM AKIWATE But I feel like there is a tendency to sort of hide behind the privacy curtain and be like, "Oh, this is private data. Let's not share information because that allows attackers to see how we do it at

home, or how the sausage is made." But chances are the attackers are pretty sophisticated. A lot of the threat actors that we have sort of tracked through a bunch of our research are really, really, really sophisticated. Just because you don't share data doesn't mean that they already don't have access to that data. So, in fact, the lack of real-world data, who it hurts the most are security researchers. And also being able to uncover real-world data. My favorite example for that is certificate transparency logs, where there is a lot of real-world data. Every time a TLS certificate gets published, it becomes public, and now it brings with it its privacy risks, but at the same time, it has unlocked a lot of value for operators, organizations being able to say, "Oh, I did not publish that TLS certificate." And in fact, I think there was a recent example of Cloudflare being like, "Oh, that TLS certificate was not issued by us." And they would not have been able to do that without some transparency and real-world data. And so that is my hot take. So second hot take of the day.

TARA WHALEN Yeah, we are totally here for all the hot takes from everyone today, so you're fully encouraged. But I also think Sarah had a point to add.

SARAH WYLD I do have a point to add, which is that my information matches your information. It's so good. So you might have noticed when looking at our stats in the blog post, that I'm sure everybody has been

reading while listening to this, that one year we had this huge jump in security-related requests. Most years we've got three, four. One year there were 43 requests. What happened there? It was one guy. There was one independent anti-phishing activist who wanted to know who owned all the domain names. And we said, "We don't think you really need to know that. Did you want to maybe just deal with the phishing?" And he said, "Yes." So we dealt with the DNS abuse without disclosing the personal data. Just as you say, you don't really need to know who owns the domain, just are they all connected? Thank you.

GAUTAM AKIWATE

And I'd also like to sort of share one thing. With researchers, one of the questions that got asked is why do we not maybe reach out to folks? And part of the reason sometimes is because we do not know who to reach out to. And some of the research that we did, the same one that uncovered operational issues, we actually reached out to Tucows, and they were super supportive, and they helped us connect the right people. But in the absence of finding those people, you have no way of fixing what are thousands of domains that are now uncovered. And I feel like part of what I hope this helps sort of bridge is this gap between researchers and the industry, where researchers are not entirely sure where we go to access this information. Is this information even public? And so what researchers sort of default to are the public sources of information or information that industry has already collated.

TARA WHALEN

Our question. We're all right on the question queue, I hope. Oh, we have a question in the room.

AZOM

Thank you. Azom, for the record. Regarding the central question, to combat online abuse and without overstepping the privacy and data protection law, can the operators have a proactive mechanism so that they can identify some of their domains which are abusing or have some compliance issue, and they can temporarily shut down, and they can have knowledge, or some tools, because the world is changing, so that it is possible to identify things, and the operator can have a step on it so that the abuse can be overlooked? Is it possible?

SARAH WYLD

Thank you. This is Sarah. It's hard to hear. So the question is, can the operators do proactive looking for abuse on the platforms? I think some do, and it depends on the nature of the operator. So for example, a hosting provider or an ISP would have different responsibilities than a domain name registrar who does not deal with the content, right? So as a registrar, we tend to more often, as I'm aware, respond to reports of abuse rather than going out and looking to see, does that domain name match a trademark, and then what are they doing on the website? And it's more appropriate for us to respond to abuse reports while a hosting provider or ISP

would be doing the proactive searching and filtering, I think. I hope that helps.

AZOM Because, see, the amount of online abuse is so huge, and the protection mechanism is very difficult after prolonged activities after the law enforcement agencies. But maybe that's a very meager percentage. So if proactive measures, I mean, the prevention, could be done, that could be one of the good steps for doing the central question.

SARAH WYLD Thank you. There are certainly levels of proactive work. It's important to make sure that we're addressing what's actually being done rather than how we think a domain name might be used in the future. And I'm sure every registrar has an acceptable use policy and terms of service that they enforce.

TARA WHALEN I think Thomas has a point to add.

SARAH WYLD Thank you.

THOMAS RICKERT Yeah. Great point, Sarah. Let me just add that I think it's worthwhile looking at the differences between what the registry can do and

what a registrar can do. So there are registries that use algorithms to find out what the likelihood of a domain name being abused is. So they would then not delegate those domain names into the DNS before they complete certain checks. So if there's a certain risk associated to a create request, then they would do a deferred delegation, as it's called, to make sure that there is no harm coming from that domain name. That's done by some ccTLD operators, but also by some gTLD registries. Then for registrars, we do know that some registrars are taking action when they get credit card chargebacks, for example. So they would then look at the domain names that have been registered in connection with that credit card chargeback. So even if a domain name is innocent, if the payer has been fraudulently using a payment method, then that might lead to the suspension of the domain names associated. And yet others are using commercial threat intelligence providers that correlate the domain names that you have under management with threat intelligence that is out there. So if they find out that there's a phishing campaign using domain names that are managed by a registrar, then they would take a look at that and, as the case may be, take proactive action before they receive an abuse report.

AZOM Thank you.

THOMAS RICKERT So some of these things happen already.

AZOM Yeah.

TARA WHALEN All right. So I know we have lots of points to get through. I wanted to thank Thomas for laying out a lot of the legal landscape to set the stage before we started the panel part. And of course, a lot of the compliance questions that people face, they're global. We have places that are operating in a lot of different jurisdictions. And specifically, I'll start with Sarah on this one and ask what the main challenges are that you face when trying to maintain compliance sort of globally, where there are different regulations and different jurisdictions.

SARAH WYLD Thank you. Yes. This is an interesting question. We're always going to follow the law that applies to us in our jurisdictions where we operate. So it's complicated if there seems to be a conflict or if there's a request for perhaps data disclosure that really does require legal process, like a warrant, but the requesting party wants to just skip over that and get the data without it. So sometimes that means that they know that they wouldn't be able to get a warrant domesticated into our jurisdiction, and they're hoping we just don't notice that. So it's really a lot of paying attention to where is the request coming from, what are they asking for, where are we,

and how do all of those things fit together? And you need to develop a pretty good body of legal knowledge. We have an excellent legal team, but it's not easy. Thank you.

PHILIPPE FOUQUART

Thank you. This is Philippe Fouquart. Just from an ISP's perspective, and just to compare what a registrar would do as opposed to what ISPs might do on their resolvers, I think as a general rule, although registrars, as Thomas said, may use things like regex, et cetera, to figure out whether a domain name may be harmful, let's put it this way, as a rule, we generally don't. However, that being said, for some keywords, as you would expect, it's always for things that are blatantly illegal under the jurisdiction in which the ISP operates, we do do things like blocking. Mindful that it's always a balancing decision as to what sort of risks that you may take, and the fact that we're not liable as to the reachability of a domain name, accessibility of a domain name, as opposed to the content that we provide access to. I hope I'm making sense. So the general rule is we don't do these things, but there are specific areas and specific content which we do block.

LARS STEFFEN

And we have another question from Steve Crocker.

STEVE CROCKER

Thank you. Can you hear me? Okay. I've just heard in a couple of cases that it all depends. You have to do a balancing test. It's a

complicated legal sort of thing. Looking at it from the requester's side, what can be done to facilitate the requester knowing what to provide, how to provide it, in order to increase the chances of a success or reduce the chance of not making unsuccessful things? And I would say the two watchwords that I have on that are consistency and clarity. So the ideal, from my point of view, is that a requester who has in mind that they want some data should be able to understand clearly how to make that request, what they're going to get back, whether or not that's going to succeed or not. And it would seem to me that improving the statistics on this would be to the advantage of everybody, not just the requester.

SARAH WYLD Thank you. This is Sarah. So there's sort of two parts to that. One part is what data to provide to make a fully formed request. And if you're submitting a request directly to the registrar, the Registrar Stakeholder Group has put together a document with a list of seven questions that should be included as the minimum required information for a disclosure request. I put the link to that document in the chat, if that's helpful. But I think the extension to that is that the concern that I think you may have is that it's not always quite predictable as to whether that will be a disclosure or a denial. And in the end, it does come down to the registrar, the data controller, reviewing the stated purpose for requesting disclosure and making a determination as to whether that does have a legitimate basis and override or outweigh the domain registrant's right to privacy. And that's very difficult to make any kind of blanket statement

about, because individual situations can be so different. There are patterns, but it's not a guarantee. And so I think basically, if the requester thinks they have a good reason to get the data, they should explain that, and it can often become a human conversation rather than a simple yes or no. I hope that helps.

GAUTAM AKIWATE

So, as a researcher, I'm typically on the requester side, and again, thinking about, so I think Sarah mentioned how it is currently, and maybe since we're at ICANN and we do things, more or less, thinking about the world we would like to be in, I think it would be helpful if we could think about ways that we could standardize what the requester is doing, and also going back to, what is the tier of request that this person is requesting? What data do they need? So it feels like my understanding, based on what we've been discussing, is that it's an all or nothing. And sometimes we don't need an all or nothing. It needn't be binary. And I don't think that distinction is sort of brought about. I think that distinction does not need to be there. We could share gradations of data, and maybe there is something that we could do where, again, going back to the registrant example, we don't need to know who exactly the registrant is because most security researchers don't care. And sort of maybe that lowers the barrier to when you can share the data and might lead to more people getting access to the data. And I think, if we can, as a community, sort of think more about what is it that we are trying to protect, and are there tiers to this? And I know we already have some form of tiers, but essentially even in

the terms of pseudonymizing, anonymizing, what have you, I think that would be a big leap forward, even in terms of having a standardized format where we can request data from. Because depending on which registrar, which registry you go to, you might need to send an email, you might need to go through their portal and click seven buttons, and then do a magic incantation before you submit. So, yeah.

STEVE CROCKER Thank you. Let me ask a follow-up. At the very beginning, there was a slide that talked about the changing environment. One of the themes in what was on that slide was the need for quick action to respond to various threats and so forth. Much of what I'm hearing in the discussion now is the need for judgment, for review, for things that take time, plus the uncertainty of it all. How do you balance, in your thought process of presenting all of this, those two forces?

THOMAS RICKERT Yeah. Thank you so much, Steve. That's a great question. And the answer, I think, and we've had a lot of discussions around this, is not really satisfactory because I think we could come up with a relatively good assessment and predictability when it comes to certain scenarios between certain service providers for certain data where we know what the jurisdictions are. Right? So if you know that a requester is asking for data based on, let's say, a trademark infringement, and that requester is sitting in the EU, and the

disclosing party is sitting in a neighboring European country, then we will probably be able to say that can be green-lighted without any effort. But globally, and that's what we're facing at ICANN, you can't anticipate exactly what the ask is. You don't know whether the legal basis or the purpose based on which the request is made is legitimate. So you need to take a look at, is the requester actually holding the rights that he or she claims to have? And then you can't disclose from each jurisdiction to each jurisdiction. So you need to check whether the requester is sitting in a jurisdiction that has an adequate level of protection. That would be a legal requirement under European laws. So what I have suggested on a couple of occasions is that ICANN could help with this by coming up with a map analyzing what the legal regimes in the various jurisdictions are, so that we can help requesters understand that if they come from a certain jurisdiction, disclosure to another jurisdiction is pretty likely or whether it's very unlikely. We can't guarantee, but we can aid this by helping people understand the legal complexities at the global level.

TARA WHALEN I think we have a question here from Santanu.

SANTANU ACHARYA Thanks. The same thing was Steve said, but in some different way. In my country, the registry is the same, internet exchange is also the same entity handling. So what is happening is that there are many registrars over there. Somebody is abiding by the KYC rule;

somebody is not abiding. So anybody can go put their email number and take a domain. So what is happening, one very famous temple is there. So you can go there either by trekking. Trekking is very tough there, so people used to book the tickets of the helicopters. And helicopters are so in demand that people don't get tickets. So now what is happening, people are putting phishing websites, because getting a website is very easy at that point of time, because in each country there is one registrar or so. And then those things are coming: the tickets are there, you can book from here. And by the time the agency, the government, comes to know this, "Yes, this is there, and this needs to be closed," it takes seven to 10 days. And by that time, he flees with millions of rupees. So I think if something can be done where ICANN, or something, can on its own take down the site rather than waiting for the agency or someone to say to the registry that the site should be closed or something. So if that can be done, I think that would be great.

GAUTAM AKIWATE Thank you. I think I understood where you were going. The audio is really difficult, so I'm having a hard time. But that something that can be done, I think a lot of that work would feed into the SSAD work that's happening right now, because that's looking at a process to authenticate requests so that the difficulty that slows down that part of the processing is gone, and then requests can be processed more quickly. So hopefully that will be useful.

TARA WHALEN Oh, we have lots we can talk about today. I felt that we didn't have enough. Oh, do we have someone on the point?

PHILIPPE FOUQUART Yeah, just a follow-up.

TARA WHALEN Oh, please. Please follow up.

PHILIPPE FOUQUART Just a follow-up question, and I know the answer should be simple. It says yes or no. But just to follow up on Steve's question as to how the random requester may improve, I don't know how to phrase that, their likeliness of having the best chance of getting the information they're looking for. Is the pointer to the guidance that, Sarah, you were referring to, available to the ICANN community through the contracted party, I don't know, their website? Or is it readily available through a pointer available on the RDAP data model, if you see what I mean? I.e., would the random requester on the Internet need to have prior knowledge of where those best practices are available? Or are the data available through WHOIS sufficient to get to that information? I hope I'm making sense.

SARAH WYLD Thank you. So I think you're asking, how does just somebody who is a random kind of person with a problem know what to do when there's a problem? Okay. So a lot of people don't know how to do a

WHOIS lookup, and that is complicated, but if they can figure out how to look up the registration data, and I know we've moved from WHOIS to RDAP, but really eventually you go on the website, and you type in the domain, and it gives you back the data in some kind of formatted manner. And then we get requests that are sent into tieredaccess@tucows.com that say, "I'm this person, and I need to know who owns this domain name. Can you please tell me?" And then we write back, and we say, "Sure. Here's our little list of seven questions. Just fill out this information so that we can assess your request properly, and then we can decide if we can tell you or not." So you don't have to be an expert to do that. Is that what you're asking?

PHILIPPE FOUQUART Sort of. You actually provide that guidance in the response that you give to the request. It's not information otherwise available. The random requester doesn't need prior knowledge. You provide it in your response to the email that they get through WHOIS.

SARAH WYLD Yes, absolutely. So if they happen to find the form or the list of questions in the first place, that's great. But if they don't, and they send in a request that we can't quite deal with, or it's confused, yeah, we write back and say, "Here's what you need to tell us so that we can process your request."

PHILIPPE FOUQUART Just to follow up, if I may. "We" is Tucows, the registrars in general, or?

SARAH WYLD Right. So at this time, we could refer to the Registration Data Policy to see exactly what's required in there, and I'm not sure if that's what we should do in this moment. Tucows, certainly, I'm speaking here on behalf of Tucows, and so my colleague answers those emails and sends back that request for more information.

TARA WHALEN Yes. Thank you for the questions and the thorough follow-up. I think this discussion is lacking a lot of acronyms, though. We haven't had enough of those.

SARAH WYLD I have the answer to the question.

TARA WHALEN Wait, we have a late-breaking answer to the question.

SARAH WYLD Okay. So there's a policy for this. Yes. The Registration Data Policy Section 10 says that registrars have to publish on their website the mechanism and format for disclosure requests. So every registrar should have it. It doesn't have to be on the homepage, but on the homepage, there's a link to where it's found that says, "This is what

you have to put into a request for us to process it." I'm sorry I didn't think of that immediately. Now I feel bad.

TARA WHALEN

No, we like having the information whenever it appears. But you derailed the critical discussion of acronyms, so why are we here otherwise? And I wanted to touch for a moment on the ADC PDP because we have Gautam here involved in the Associated Domain Checks PDP on behalf of the SSAC, one of our representatives. And a quick summary for the people who are not following this very closely: I got a little bit from the charter. So this PDP seeks to create an obligation for registrars to investigate other domains associated with a customer account or registrant, where at least one domain of that registrant is found to be engaged in DNS abuse, as defined in the RAA. The associated domain check would seek to solve a gap by requiring all registrars to cross-check within the registrar's portfolio the known abusive domains to others connected to the same customer account, registrant email address, or other pieces of information. And one of the questions identified in the charter is: what data access and privacy safeguards are necessary to protect both registrants and registrars during associated domain checks? Now, I know this is only early days for this, but I wondered, Gautam, did you have any thoughts about this question?

GAUTAM AKIWATE

So one of the things that I was thinking of as folks were asking their questions about, oh, there are these phishing sites that sort of crop

up, what can operators do? And this seems like one of the ways that we can sort of shorten the time to which the abuse can get limited, or the uptime is limited, where the act of flagging one domain might sort of have a cascading effect through and through. And as you said, it's still early days about how do we navigate this issue, because I think there are a couple of complicating factors where if a domain gets flagged, and there are associated domains, but those associated domains are not being used currently for abuse, what does it mean? And I think there are a lot of questions like that that need to get answered. But from a privacy perspective, I think there have been a couple of questions about if somebody gets it wrong, how do you fix that, and what are the mechanisms to fix that? And then also correspondingly, is there a privacy risk when you're doing an ADC check? Does it mean that accidentally something that you were doing on a personal basis also gets taken down because reasons? So I think there are a couple of unexplored areas there. I'm not a lawyer, so it makes things challenging when they say "reasonable," and I'm like, "I don't understand what reasonable means." But clearly, the lawyers have an idea about what reasonable is. And I wondered if Thomas has any thoughts on some of the ADC work that's been going on, given that he's the lawyer on the panel.

THOMAS RICKERT I think that we're making very good progress, and I think that the ADC is a great tool. Unlike other participants of the group, I think that the collateral damage caused by ADCs is zero for the

registrants involved because at that point, you're just checking whether you have other domain names in your portfolio that might cause harm. And the mitigation is the next step. The first point in time when there could be harm for a registrant is when the domain name is actually being taken down. But I have hopes that the ADC will be a success. But I should caution that the ADC becoming a policy in itself will not yield huge results because it's difficult to, if you just look at the policy itself that requires registrars to check whether they have associated domains, that can have two consequences. If there are almost no ADCs that are being conducted, does that mean that the policy is ineffective, or does it mean that there is no harm, right? Or that the perpetrators have become more sophisticated and spread their portfolio across different registrars so that they go undetected? Or if we have a lot of ADCs, does that mean that we identify a lot of patterns of abuse and become more effective? So I think it will be important, and this is something that we're pushing for, that not only the contracted parties, but also ICANN org and OCTO work together, that OCTO looks at the overall landscape, looks at what campaigns of criminal activity are going on, what registrars are being used for that purpose, and then audits these registrars to check whether they have fulfilled their duties in following up on cases that have been brought to their knowledge. And we need ICANN org to sufficiently resource ICANN Compliance to go after the bad actors so that they can improve their game and become part of the solution rather than the problem.

GAUTAM AKIWATE

So one of the things that Thomas's answer reminded me was the fact that threat actors might now spread their load across different registrars. And so one of the things that got punted was the fact that how do you do cross-registrar intelligence? And this is one of those places where the privacy aspect starts. Now, how do you balance privacy and security? And I said I'm not going to use the word balancing, but I did. Because in this case, it actually does. But again, to my point, there is a way where registrars could, and there has been, so if folks are interested, SSAC is going to talk about some of these blinded identifiers, like mechanisms in which registrars could potentially use a blinded identifier which could track the same registrants across different registrars. And so we have the same identifier across. Now, there is a lot of work that goes into trying to de-anonymize what have you, so we haven't really sort of figured it out completely, but that is one of those areas, I think, where this privacy-security debate is going to sort of play out next. And I do think that for us to be completely effective with ADC, one of the things that we'll eventually have to sort of solve is how do we do this cross-registrar intelligence, and how do we share without, again, going back to my favorite, you don't need to know who the exact registrant is, except that this is the same person who has been registering domains across these different registrars. So. Thomas has a...

THOMAS RICKERT: Yeah, just a quick follow-up. I think that one aspect that we seem to be neglecting when we are here, all coming from this community being locked into these windowless rooms, is that we think we can do this on our own. And I think that not every solution to the issues lies with ICANN, right? So I would just point you to this initiative called the Internet Infrastructure Forum that tries to bring together not only registries and registrars, but also hosting companies, CDNs, and others. And they are currently working on a pilot to allow for more efficient threat intelligence sharing across different actors up and down the stack, because that's, I guess, key. And this is a joint responsibility that we need to explain to the outside world, that ICANN is just able to do that much, that there's much more to it in this ecosystem, and that all the parties need to work together more efficiently.

TARA WHALEN: I know that we're now down to the last few minutes of the session, so I'm looking to our organizer. Do we have any questions from the chat that we want to pull forth into the room?

GAUTAM AKIWATE: I don't see it.

TARA WHALEN: Okay. No one is on the queue.

GAUTAM AKIWATE

I was going to do a quick plug for the DNS Transparency Work Party. So Raphael and I, who is in the audience right now, are co-chairs for this SSAC Work Party called DNS Transparency, which essentially is an attempt at trying to log different DNS configurations that are happening at different levels, at the registrar and then at the registry. And this is one of those places where the privacy and security debates sort of come forth, is now if you're logging every DNS configuration change, what are some of the risks associated with it? And part of the motivation behind this effort has been, the effort started as a result of hijacking risks where government organizations and a lot of nation-states were targeting registrars and registries in order to sort of change name servers for short durations of time, and get TLS certificates because now TLS certificates you can get through domain validation. And so what started out as an idea about, oh, let's log DNS configuration changes so that an organization can audit its log and be like, "Oh, this was a change that we did not authorize," similar to certificate transparency logs. And a bunch of the community was like, "Oh, actually, when you do this logging, we can also identify a bunch of abuse. We can identify shared infrastructure, we can identify patterns." But then also there is this question of, how do we sort of make sure that this is behind access control? What is the kind of access control you do for this kind of data? Certificate transparency is public. Can we sort of go to the same extreme, though, making all of this data public? And that is a question that we are trying to answer in SSAC. And if folks are interested, this ICANN, it's already too late, because we had our work party meeting just before in the

previous session. But if folks are interested in understanding what that is and how that might help them, we are happy to answer questions. Yeah.

TARA WHALEN

Yes. Thank you, Gautam. I like all the reminders of how we need to solve these problems collectively and with collaboration. So thank you for the invitation. I think maybe with that, we will wrap our part of the panel.

LARS STEFFEN

Thank you very much. And thank you very much for providing your insights and sharing your details with us. And thank you also for emphasizing the working group and also referring to the Internet Infrastructure Forum that Thomas has just mentioned. So there are currently different working parties, or different working groups, I'm sorry, and initiatives that are discussing the sharing of information and intelligence across the stack. So it's not only about registrant data, it's not only about domain names, it's not only about ICANN. So there are different fora currently in the stage of being established where we open up the discussion involving other providers across the stack, because it's relevant to include the entire stack if we want to make a difference and want to be effective and want to be also fast in the respective responses and to be meaningful. So with this, I would like to thank everyone in the room and also online, and also, of course, our excellent panel and also Thomas, who have taken the effort to prepare all this. It's not

only just being here for the session, it's also all the time and effort that went into the preparation. So thank you very much. And thank you also, as always, to the staff in the background, to the interpreters for being with us and to provide their excellent support. And with this, I would like to close the session. Please visit ispcp.info after the summer break, where we will announce the next series of webinars starting in September. And hopefully see you again at the next ICANN meeting or online at our next session. Thank you very much.

DEVAN REED Please end the recording. Thank you.

[END OF TRANSCRIPTION]