ICANN81 | AGM – GDS: PPSAI IRT Work Session
Thursday, November 14, 2024 – 9:00 to 10:00 TRT

LEON GRUNDMANN: Hello and welcome to the PPSAI IRT 9th session this 14th of November, 2024 at ICANN81 in Istanbul at 6 a.m. UTC and 9 a.m. local time. My name is Leon Grundmann and I am the remote participation manager for this session. Please note that this session is recorded and is governed by the ICANN Expected Standards of Behavior and the ICANN Community Anti-Harassment Policy. To ensure the transparency of participation in ICANN's multi-stakeholder model, we ask that remote participants sign into Zoom sessions using your full name.

You may be removed from the session if you do not sign in using your full name. If you would like to speak during the session, please raise your hand in Zoom or alternatively in room, in person. We'll do our best to cycle in between in person and remote participants. When called upon, participants will be given permission to unmute in Zoom. Please do state your name for the record when speaking and please do speak at a reasonable pace. I'll now hand the floor over to Dennis Chang to kick us off.

DENNIS CHANG: Thank you, Leon. Welcome, everyone. Those of you seated at the table, please use the microphone that's in front of you. And those of you in the back, you're welcome to join us at the table. There's plenty of room.

Make yourself comfortable. Let's get started. Alex, next. It's not working. Okay.

So what we'll do is I'll give you a very quick background and we have three speakers who's going to share their experience on privacy proxy. And at the end, we'll leave some time for the community Q&A. So, this policy started, well, many years ago. And we will be going through at this meeting, sharing some industries, what we are experiencing today. We have, as of today, 55 IRT members. We have a couple of GNSO liaisons and stakeholder representative and alternatives, as well as individual contributors.

And we have so far reviewed 21 recommendations. That actually resulted in about 100 comments that we were addressing. And we had to do that because when we started this work back in Kigali, this was a resuming of the implementation activity that was paused in 2019. So, we wanted to look at the recommendation's language from the scratch and a fresh start.

So, now we are here. What we are going to do today is to hear from our three speakers who are using the privacy proxy services. And we will hear how they're using it and learn from it so that we may use the information to design our implementation model and craft the policy. Just so that you know, the following slides that we have here are from the speakers themselves, and it's not from the ICANN org. So, we don't mean to be saying that this are the way you should do things or the way the policy is designed to do things, but it's simply a look at the current

market space and how things are working. So, let me turn it over to our first speaker, Margie. Go ahead, Margie.

MARGIE MILAM: Hello, everyone. I'm Margie Milam. I'm with Meta Platforms, and I'm also the business constituency representative to this group. I've been at Meta for about seven years, and I'm on the domains, trademarks, and marketing team in the legal department. So, that gives you a little bit of a perspective of how I sit in the organization.

My responsibilities at Meta include domain name policy, which is why you all see me here, and also off-platform enforcement and litigation. And today I'm going to be talking a little bit about our perspective as a social media platform with over 3 billion daily users on our products. You know our products, Facebook, Instagram, WhatsApp. And because we are so large, we see a lot of the abuse trends probably before most people do.

And so, the perspective I'll be sharing is from the scale issue because we typically deal with abuse. We deal with thousands of brand infringements every year, and probably hundreds of thousands of phishing attacks against our major brands. Prior to joining Facebook, I was a vice president at ICANN in the strategic initiatives department, and I was also a senior policy counselor working on WHOIS issues, privacy proxy when I was at ICANN, as well as the RAA amendments. So, that's why when on this group you'll hear me talk about some of the history behind how we got here. And before that I was general counsel

of marketing monitor, so I've been in this space for quite a while and dealing with the privacy proxy issues.

So, from the perspective of a requester, this policy is a very important improvement to the DNS ecosystem. We see a growing trend in the use of privacy and proxy services in particular for abusive domain names. The statistic that you see on that slide shows that 65% of abusively registered domain names use privacy proxy services, which is a significant amount, and it's actually in greater proportion than we see in other domain names. And the other thing we see is that the usage of privacy proxy services has increased dramatically since 2021, when it was something like 29%. So, it's gone up a lot.

And I think the logic behind why the use of privacy proxy services has increased is because of the GDPR and the changes in the WHOIS policy. What we see is that many registrars by default apply privacy proxy services to all the registrations. And so, what that does is it makes it increasingly challenging to find out who is behind some of the abuse that's targeting our brands, and particularly our customers and the public that we're trying to protect. We often need to access that information to be able to investigate fraud and abuse.

What we find is that many privacy and proxy providers, they are not contactable and they do not respond to requests. Now, certainly that's not true of all privacy proxy providers. There's definitely ones that do, but at the point of having a policy is to apply the standard across the board to all privacy proxy providers. We also note that we've seen in practice that there's a very difficult time trying to find out abuse points

of contact or even understanding the abuse procedures that privacy and proxy providers use. And that makes it very difficult to do the kind of investigative work that we need to do when we're trying to protect our customers from fraud and abuse.

What we see when we do try to make requests is that the disclosure rates are quite dismal. If you take a look at the statistics that Tracer publishes, they publish them quarterly on the types of requests that they make. We see that the rates have dropped dramatically even this year, something like 51% in January to about 4% in September. If you look on their website and you'll see a gradual decline of successful reveals. That is problematic when you're really trying to protect the public from this type of abuse.

To put it in context, I can give you a few examples of domain names that show you the types of problems we see. An email like 40facebook.com and that's spelled correctly or 40instagram.com would be denied when there's a privacy and proxy service involved. As a company trying to do what they can to protect their users, it makes it very difficult to be able to ensure that we're taking action to protect our customers. Even a phishing domain name is like aa-whatsapp.com. We won't even get a response from a proxy provider even when we have a phishing attack and we show proof of phishing.

That's the scenario that we're dealing with every day. It's a non-stop process that we're dealing with in trying to fight the kinds of abuse. That's why we think this particular policy would be a good step in solving the problems. It won't solve all of them for sure but it'll certainly

help in terms of investigations. As a result, what we end up doing when we can't get things down or we can't investigate, we will do UDRP filings. If you take a look at the statistics from WIPO, you'll see that the number of UDRP filings has gone up over the years. And even that sometimes is problematic because when you do file a UDRP, there are circumstances when a proxy provider will not reveal. You still will never know who the customer was behind the bad domain name.

The other thing we find is that many privacy proxy providers are affiliated with major registrars. It's really interesting because even though there's usually a privacy proxy provider that's associated with a registrar, oftentimes they go through great lengths to make it seem like they're not related. Oftentimes, the procedures that they apply will be very different from what they would apply for non-privacy proxy domains. The interesting thing is we even see different reveal rates and takedown success if we're dealing with a privacy proxy provider that's affiliated with a major registrar.

There's a lot of inconsistency going on. I think that the types of things that we're talking about in this group and the policies that we're trying to implement will make it much more consistent across the board. The other thing I'd like to point out is that we do see inconsistent usage of terminology. Oftentimes, we'll see privacy and proxy providers use various terms that are inconsistent with what the RAA says and what the policy says.

For example, if a company might call themselves a privacy service, but then when you look at the WHOIS record and you look at the registrant

field, you would see their information in the registrant field. That's inconsistent with what a privacy service should show in the WHOIS record. It should show the customer's name in the registrant field or rejected for privacy or something like that if it's rejected for GDPR purposes. That's one of the things I think as this group moves forward, we can really make it very clear as to when you use a proxy service and when you describe something as a privacy service, but the nomenclature that the services use might actually be inconsistent with the policy. Next slide, please.

I think that's pretty much what I wanted to cover. Unfortunately, I have to leave for a flight. I'm not going to be able to stick around for the whole session here, but thank you very much for letting me share my perspective. Patrick and others can talk about business issues if there are any questions when I leave. Thank you.

For some reason, I thought the slide was gone. The reason why I raised this was I went through the report and I highlighted some of the things that are in there and why it would be helpful for the business users. As I mentioned, the labeling issue, right? That would make it very clear how a proxy service describes itself and the labeling would help too because sometimes business users don't even know they're dealing with a proxy service. We've found that quite a bit that when we're trying to investigate a particular domain it's not even clear from looking at the WHOIS record that we're dealing with a proxy service.

We'll also see what we call double redaction. It'll be redacted for privacy and then when you ask for a reveal or you file a UDRP, you find

out that it's a proxy service. A proxy service will redact its information in the WHOIS record, which makes it very, very difficult. We will also see situations where it's triple redacted if you think about it from that perspective. You'd have it redacted for privacy, then you'd find out it's a proxy service, and then later on you find out that a registrar might actually be owning the domain name directly through one of its affiliates. It's that non-transparency that I think would be very useful to clarify through this policy implementation.

We also will definitely appreciate the requirement to relay the communication to the customer of the proxy service or the privacy service because oftentimes when a domain name is registered perhaps inadvertently or the customer doesn't really appreciate why they shouldn't be registering that domain name, the ability to relay the communications actually helps resolve the issue without ever having to go to a UDRP. That would be very helpful. Then the other points that I think that are highlighted here are all things that I think would help from a consumer protection point of view and really help the requester community understand the rules and the framework that would apply to requests.

GABRIEL ANDREWS: Hi. Noting that you're going to leave, I can ask a very quick question. With the double redaction that you just described where you would first see redacted for privacy or similar, you file the request and then you get back information point to a proxy service, if I understood you. Was that

an unaffiliated proxy service or affiliated or mixtures of both that you've encountered?

MARGIE MILAM: They're usually affiliated. It's pretty clear from-- I mean, most of the registrars in the room know who their affiliated proxy providers are. Most of the time, it's the case that it's an affiliate. The interesting thing is because it is affiliated, it's usually the same people that are working the abuse desks and responding to the requests. It's really interesting that we're unable to have the same reaction kind of from essentially the same entity because it's the same people that are looking at the requests and responding to it.

Let me see if there's anything else I wanted to highlight here. The last thing I think I wanted to highlight was that, I think we're debating this in this group quite a bit, whether it's important to have a direct contract or not. We're talking about the actual accreditation agreement in the context of the implementation. It would be, I think, very difficult to implement all of these things if you didn't have a contract because it would essentially have to flow through from the registration agreement to the proxy providers. I don't think that would be quite as enforceable and give the kind of improvement to the ecosystem if it was more of a flow through as opposed to an actual contract. That's why the accreditation aspect of it would be very helpful.

If you look ahead to the implementation of NIS2, NIS2 applies to privacy proxy providers. There's certain requirements related to verification and disclosure and all of that that would apply, and I believe that it

would be easier for them to comply if there was an accreditation program. Because there are certainly situations where privacy proxy providers are not related to registrars. That's the scenario where I think it would be particularly important to have contracts.

REG LEVY: To follow up on Gabe's question, sorry, this is Reg Levy from Tucows. When a registrar uses their own privacy service in the WHOIS and redacts it, that is against ICANN policy, so please report them. I'd also like to know more about the three-level proxy that you talked about where it sounds like a registrar owns the domain in their own right, then uses their privacy service and then also is infringing on yours.

MARGIE MILAM: Yes. An example of that would be in the expiration time, expiration period. Domain name is about to expire. Rather than letting it drop and delete through the process, you'll see a registrar transfer it in their own name so that they can resell it on the secondary market. Then in that scenario, that's often redacted through a proxy. And so, that's a scenario I've seen in other situations.

DENNIS CHANG: Anybody else? I'll ask a question, Margie. Have you encountered any unaffiliated privacy proxy service provider? And if you have, how did you able to manage your communications and get your information?

MARGIE MILAM: It's difficult to know how many are accredited or how many are affiliated with an accredited registrar because there's no list of it. And that's one of the things that would be helpful here is to be able to do that. So, it's hard to say, but there are definitely proxy or privacy providers that are unreachable and have no procedures for dealing with disclosure requests or even takedown requests.

DENNIS CHANG: So, how did you resolve it when you cannot, and that's what I was wondering.

MARGIE MILAM: You can't. I mean, there's many, many domain names that stay because you just can't. You couldn't, your options are UDRP and there's only so many UDRPs you can do when you're dealing with thousands of domain names that are infringing at any time. You just do the math, right? It's prohibitively expensive to file a UDRP for every domain name that infringes. So, you essentially reach out to the posting provider if there is one. And if you can't file a UDRP, you consider other forms of legal action if that's available or try other ways to address it.

LEON GRUNDMANN: Dennis, just flagging, we have one or two questions in the chat. I see two questions from Farzaneh Badi. Would you like to speak to that, or would you like me to read your question?

FARZANEH BADIEI: No, I'm sorry. I had like a few questions on that, but I came in late. I'm sorry about that. I don't understand what consumer protection for customers of privacy practices services is. And also, I don't understand what sort of takedowns, as Margie says, like privacy practices services do, if they do any. Another thing is that I also think that if the trademark owner wants to assert their trademark, I think they should go through the route of UDRP and pay for it and get their domain name back.

MARGIE MILAM: Thank you, Farzaneh. Regarding the customer protection, I missed that one. So, oftentimes, customers of privacy proxy providers don't understand the rules that apply to them, right? For example, when is it when a service might reveal the information? What happens if the provider goes out of business? Is there information covered by escrow? So, a lot of those things are the kinds of consumer protection angle for the customers of privacy proxy services that are useful. And the policy talks about these services having published their policies and procedures. So, that's why I flagged that as businesses are often also customers of privacy proxy services that is helpful to have that type of consumer protection.

DENNIS CHANG: Are there any other questions? If not, we'll move on to the next speaker. And thank you, Margie.

MARGIE MILAM: Thank you.

DENNIS CHANG: Owen, you're up.

OWEN SMIGELSKI: Thanks, Dennis. Hi, everyone. My name is Owen Smigelski, and I am with Registrar Namecheap, and we also have a newer accreditation spaceship. So, I've been with Namecheap since 2018, and prior to that, I spent seven years with ICANN Contractual Compliance, where I was responsible for setting up the 2013 RAA compliance program. So, I'll be speaking in part of my experience with that, with helping get all that stuff set up.

So, our registrar utilizes a privacy service called Withheld for Privacy ehf. It is an entity based in Iceland, and we chose that because we wanted an entity that would be subject to the more stringent protections of the European Economic Area under the GDPR, as opposed to something that was based within the United States or another jurisdiction. So, I'm going to be speaking a little bit more to some of the things about it currently, about what I've seen from now versus what was, say, 10 years ago when this whole thing came into place. Next slide, please.

So, just a little history about privacy proxy services and how ICANN came to deal with them. A lot of what we see in the RAA or the Registrar Accreditation Agreement, some of it is dictated by ICANN policy, but then also part of it is in reaction to what registrars are doing in the field. So, the 2001 RAA I had no references to privacy proxy services. I must

confess I was not involved in ICANN at that time, although I did have a domain name, but my domain name had my own personal contact information for my home address there.

So, the first time, the 2009 RAA was starting to make references to privacy proxy services, and the only thing in there that it did with regards to privacy proxy services was Section 3.4.1, which said that a registrar must include underlying customer data along with the public registration data for data escrow purposes, or a conspicuous notice that indicated the underlying data was not being escrowed.

So, what that means, if somebody is using a privacy or proxy service, when you look them up in the WHOIS, and I'll use WHOIS because that's what it was called back then, when you look it up in the WHOIS, you would see, say, domains by proxy. So, the underlying, either the beneficial user, if it was a proxy service, or the actual registrant, it was a privacy service, that data would also have to be escrowed, and then that would have to, or if not, there'd have to be a notice stating that it was not doing that.

And this was a reaction to, some people may have heard of RegistrarFly, which was a registrar that exploded around this time, and there were some issues with data going missing and registrants not being contactable. The other reference to it was that resellers must also do this, so there couldn't be a way to get around not escrowing those underlying data or making a notice that it was not being escrowed. And that was all that was in there.

Next slide is what happened was the 2013 RAA. And a lot of this came in response to wanting to get a new accreditation agreement with the new gTLD program. And it actually included a specification on privacy and proxy registration. What I'm going to be citing here are some different definitions from there. This is actually stuff that I'm quoting directly from the RAA. The creation of this privacy proxy specification was because there wanted to be some type of rules and requirements for privacy proxy providers.

However, there wasn't really enough time as part of the negotiation process for the 2013 RAA to come up with a detailed robust policy. That specification was sort of what the general business practice was, or some of the best practices that most registrars at the time were doing, and so it's reflective of how it was at that time with the understanding that there would be a later policy initiative, which we are all part of now.

This is when the first distinction was really made. And again, this is RAA definition, not necessarily practice or understanding by people in the real world, because the RAA is not the real world. And so a privacy service is where a registered name is registered to the beneficial user, but has ultimate reliable contact information. So when you would look it up you would see the person's name as the registrant, and then it would identify have some information identifying it as a privacy service, and then accurate contact detail, which would either forward or an email or something along those lines, just so that the person's private information, their home address or whatever, was not revealed.

And then the distinction with a proxy service was where the proxy service would be the registered name holder, and then license use of the registered name to the privacy proxy customer, in order to use that. You know some of those terms are defined in there, like what a PP customer is. So technically the registrant would be the proxy service, whereas with a privacy service the actual registrant would be the person who had registered the domain name. Next slide please.

Here are two examples of how you would be able to tell the difference between a proxy service and a privacy service. And I first did this exercise back in, goodness, I don't know, 2014 or so, when I was at ICANN trying to help train staff who were coming on to join our team. And I wanted to find examples of proxy services and privacy service and how they would look in the WHOIS output. For the most part, again, this is 2014, 2015, for the very most part of all domain names, we're not using any type of privacy or proxy service. It was all personally identifiable information that was out there.

The main ones that you would see were proxy providers, where you would see up at the top, where you see the registrant name. The registered name would be the actual entity, the proxy provider. Again, these are illustrative examples. These are not exact examples. And then underneath it would have the contact information. And then you'd be able to contact the customer through that proxy service.

I had a really difficult time trying to find a privacy service back in the day, as an example. You see down below where this is an existing example, something would be today, because although a lot of

registrars did use privacy and proxy services as a way to comply with the GDPR and the temporary specification and other privacy regimes, technically you'd have to put the customer's name there and the registrant's name. But since that's a violation, you then redact it.

So I know Margie had mentioned about the difficulty about knowing whether something is privacy or proxy. I'm not sure I share that, because under ICANN requirements, a privacy or proxy service must have its full information in the RDDS output. So, that's why you see street, city, everything like that, which you would not see if it was redacted for an individual's use.

So that second example is a privacy service. I remember when I was trying to dig about this, I can't remember, but there was some EU-based registrar using a privacy service. When I prepared for this presentation, I started looking around and looking up all of what I thought had previously been proxy services, and it looks like now as the way that people are presenting or registrars are presenting it in the registration data output, is that they all have moved over to providing privacy services as opposed to proxy services. Next slide.

And this is the reason why I think a lot of registrars are doing that, because RAA Section 3.7.7.3, and because it's italics, that's exact wording in there. It says registered name holder licensing use, so that's a proxy service, according to its provision to accept liability unless you disclose the contact information of the licensee within seven days of a request for that information. And then RAA requires all registrars to include that provision in the registration agreements.

So what that means is a proxy service does not reveal the underlying customer within seven days, the proxy service is liable for anything that that registrant might be doing. Because of that, we've seen a lot of registrars move to privacy services, and that's how that earlier example where the name is redacted, the registrant name is redacted, and then you see the customer information is there. Next slide, please.

So, that was it for me, so I'm happy to pause here and see if there's any questions.

PAUL MCGRADY: Thanks so much. I'm Paul McGrady. Is there anything in the policy that we're attempting to implement that would require a labeling of the difference between privacy or proxy so that people don't have to know everything that you know in order to determine which one it is? Thanks.

OWEN SMIGELSKI: So, while I was on the working group as ICANN staff, my recollection is there were discussions about doing that, but that would require a change to WHOIS at the time, WHOIS output, and whether adding a field or a flag or something like that was considered, I think, ultimately rejected by the working group.

JOTHAN FRAKES: Hi, Jothan Frakes, for the record. I don't know if I shift this way. I'm on the camera. Hi, everybody. Anyway, yeah, so I saw-- can you go back one slide? I try to use radical empathy as we carve our path forward

here, and with these two examples, I don't see the word proxy anywhere in the second example. I'm not trying to proxy shame you here, but I can understand. I have empathy for the public who are looking and trying to parse between does 3773 apply or doesn't it apply? It's probably pretty confusing for people. We may need to think about how to at very least label that so that people understand it better. Thank you.

OWEN SMIGELSKI: Sure. Jothan, also to touch on that as well too, back when I've done this research, just because it says privacy or it says proxy in the name does not mean that it is one or the other. Because I remember looking once. There was a privacy, they called it privacy service or whatever, and it was quite clearly a proxy service, and domains by proxy is most definitely, it looks like it's acting like a privacy service. So, just because it's called something doesn't necessarily mean it's that, but I agree it is confusing.

JOHN MCCABE: John McCabe for the record. I have a question, that same question because I look here on-- well, it was on Agenda 4, I guess. The top one says you have it labeled as proxy service, and the bottom one is labeled as privacy service, but in the registrant organization it says it's private registration, and I don't understand why it wouldn't say it's a proxy registration. That's for clarity purposes. Thank you.

OWEN SMIGELSKI: Again, this is just an example. That's not an actual thing we do. What you see on the bottom, privacy services, that's an actual, that's how we actually do provide it right now for domains that are registered through Namecheap and Spaceship. Again, that top one was an example, but if you see the registrant name, there's the entity there, and then below whatever's in the organization field, you can copy it again or something. I was not trying to give an example that would show absolutely everything, but, yeah, it is something that could be confusing for those who are not in the field.

DENNIS CHANG: Next we have Gabe Andrews online.

GABRIEL ANDREWS: This is Gabriel Andrews for the record. I was just trying to use the queue. So, Owen, thank you, first of all, for walking through this. I think this is, even for someone like me, I've been here five years, not as long as you, still very informative. I appreciate the effort that goes into it. I'm curious if you could also speak to what difference, if any, exists in the escrowed information that's passed to ICANN for escrow purposes when there's a privacy service versus a proxy service versus neither.

OWEN SMIGELSKI: I might have to defer to Amanda here because she's compliance, but because I think it is now required that you do both the public registration data as well as the underlying customer information. I don't think there's an option to opt out of that.

AMANDA ROSE: This is for escrow?

OWEN SMIGELSKI: Escrow.

AMANDA ROSE: Correct.

OWEN SMIGELSKI: Yeah, yeah, that's correct. So, you do have to do the public and the underlying now. It's not an optional thing.

GABRIEL ANDREWS: If I may clarify too, is the term that you use then underlying customer?

AMANDA ROSE: There's probably several different ways, but yes, underlying customer data or the actual definition and the specification would be the privacy customer or the proxy customer. So, other terms, beneficial user, a lot of these are overlapping and often used together, but essentially all the same thing.

GABRIEL ANDREWS: Copy, okay. The reason I'm asking too is just to try to help us find the right terminology, the right times and so forth, noting that I've also seen a lot of overlap. So, thank you for that.

AMANDA ROSE: I think in the recommendations they use beneficial user and there's one other term as well. So, that can be looked at.

DENNIS CHANG: John?

JOHN MCELWAINE: John McElwaine for the record. Can we go to the slide about 3.7.7.3? Not sure which one that was. So, under the 3.7.7.3, where it says that there would be liability for the harm caused, who is the party that can bring that? Because hadn't there been some cases that say a brand owner can't bring an action, citing that they're a third-party beneficiary of that?

OWEN SMIGELSKI: I have to be delicate how I speak about this because our departed Margie, her company and my company had some discussions about this in court perhaps. So, I really can't speak to that, but I do know that that has been used in some litigation. Your mileage may vary.

JOHN MCELWAINE: Well, I guess maybe in general, was it supposed to be the-- when the policy was putting together, was it supposed to be third parties or is it supposed to be you're liable to ICANN compliance? I'm just confused.

OWEN SMIGELSKI: Again, I think this wording comes from the 2009 RAA. No, actually, this would be from the 2013 RAA. I was not at the negotiation tables for that. So, I don't know. And I don't think we have anybody. Well, Volker's here. He helped negotiate it. So, unless he can give some guidance, I don't know.

JOTHAN FRAKES: Hi, again. This is Jothan Frakes. Can you go back one slide one more time, Owen, replaying the oldies? So, I note in this, one of the things that I've heard, and it really has given me some concern, is that we would use some form of regular expression or some sort of detection while we're in some interim period to determine if things are privacy proxy of third parties to identify them. And as I look at this, I really have challenges. I see the word privacy, but I don't know if I necessarily would know to allocate this, because I've seen privacy services that they don't have privacy or proxy or other things in the name.

These would probably be detected if they were third party or if, let's say, your registrar, somebody transferred from your registrar but kept your privacy services, assuming accreditation stuff happens. I'd be able to detect that, but I just am concerned about regular expression type of ways to determine third party privacy proxy providers. This is very clear

line if you see it in the organization or the registrant name, but you don't see that very thoroughly throughout. So, I just wanted to point that out as part of the discussions. We don't want to use that as a technique because it might be a bit too ham-fisted. Thank you.

DENNIS CHANG: Roger?

ROGER CARNEY: Thanks. Just to clarify a statement that was made earlier, domains by proxy does state domains by proxy in the organization of every record. So, I think it's fairly clear that it's a proxy service. So, thank you.

OWEN SMIGELSKI: Apologies for that. I didn't mean to speak on behalf of another registrar. It's a privacy proxy service.

GABRIEL ANDREWS: Hi. This is Gabriel again for the record. Also, I just want to highlight that the current way that this is implemented, all of these fields are user editable. So, if you're a bad guy that's just trying to cause confusion for folks like me, it's not very hard to lie and point to a proxy service and cause us to spin our wheels needlessly for 30 days, two months to send a legal process ultimately to a place that tells us that it's entirely wrong. And so, some sort of authenticated mechanism to confirm that a proxy is in place that is not under the control of a potential bad guy, it'd be

fantastic, especially if it's the registrar or testing that their affiliated proxy is in play. That'd be phenomenal.

OWEN SMIGELSKI: I could just respond to that from a Namecheap perspective. In theory, somebody could do that, but they would have to enable that they would be-- So, by default, you get the privacy service. If you wanted to remove it, you have to go through a disclaimer saying you're doing it, and then you would copy and put all the information in there. I mean, it's multiple steps, but it wouldn't be something that somebody could just easily do. But yeah, somebody could copy that data and go to, say, GoDaddy and still have the fake, the old data from our service.

GABRIEL ANDREWS: Yeah, and I'm not going to name names here, but I know how difficult it is because I've done this just to test with a few different registrars pointing to other registrars' proxy services, and I know it is feasible. But I would really like to see a productive effort to make it be authenticated by the registrars themselves rather than user text field generated.

DENNIS CHANG: Let's go to Reg now, and we can come back after Reg for any follow-up questions.

REG LEVY: Thanks. Hi, this is Reg Levy. I'm Associate General Counsel for Domains for Tucows. The Tucows family of registrars consists of four registrars,

Enom, Tucows, EPAG, and ASCIO, and we have two affiliated privacy services, Contact Privacy and WHOIS Privacy Protect. The Contact Privacy is affiliated with Tucows. WHOIS Privacy Protect with Enom. Next slide, please.

Sorry, I'm going to try to speed this up a bit because I think we used a bit more time earlier. I want to be clear what we're talking about. We're talking about the release of registrant data. There's been a move to calling it RNH data, so I'm going to call them the RNH. There's something happening on the domain, and a third party wants to know who is responsible.

The RNH is responsible contractually for all content on that domain. They might purchase a domain through a reseller who would hold the RNH data in addition to providing it to the registrar. They may pay a registrar-affiliated privacy service, and so the registrar and the privacy service have that RNH data, or they may buy the domain directly from a registrar, in which case the registrar has the RNH data. You may notice that in all cases, the registrar has the RNH data. The registrar can release that data using its legal advice and local laws to appropriate parties who want to know that RNH data. Next slide, please.

Tucows, which we sometimes call up an SRS, and Enom are both Tucows companies. They have and disclose to ICANN registrar-affiliated privacy services. OpenSRS's privacy service is called Contact Privacy, and Enom's is called WhoIsPrivacyProtect. You may note that I'm using terms differently from those defined at the top of the presentation, and that's because the terms that I'm using reflect reality

rather than the definitions that were created a number of years ago. Again, the registrar holds RNH data. We publish the privacy service information in the public WHOIS, and we only release RNH data upon receipt of adequate due process. Next slide, please.

Tucows registrars also have reseller networks for parties for whom becoming an ICANN-accredited registrar is too onerous for their business model. I want to remind everyone of the first slide. In the case where domains are registered through a reseller, the registrar has RNH data, and so does the reseller. Some resellers choose to operate as proxy providers. In these cases, they accept full responsibility for anything that the domain is used for.

They are the RNH. Their information may or may not be published in the WHOIS. The information that the registrar can disclose upon request, including under penalty of law, is only that of the RNH. For proxy resellers, that is also the information of the reseller because the reseller is the RNH. If there is a customer of the reseller, the registrar does not have that information.

As a reseller-based registrar, Tucows regularly deals with registrants whose resellers have failed them in some way, and it is our pleasure and responsibility to help them, which we do if they are the registrant. If someone comes to us and claims that they own tucows.com but they aren't the RNH, we cannot help them because they are not the RNH.

Some of our resellers have portfolios of domains that belong to them directly. They may look like proxy resellers, but are in fact domain investors taking advantage of our wholesale pricing. We can't just tell

by looking at a reseller, at a reseller's account, or at a particular domain whether there is a proxy situation, and again, a reseller that acts as a proxy takes full responsibility for the use of that domain. If there is something going on, on a domain that someone doesn't like, they can pursue legal and criminal action against the RNH, against the proxy, against the reseller. Next slide, please.

Sometimes someone will buy a domain for someone else. Someone's sister doesn't know how to use computers and wants a website for her art. Someone's drunk friend has a brilliant idea of an evening. Someone's client is about to publish a billion-dollar blockbuster and doesn't want anyone to know that they're buying a domain name before it's announced. Again, the registrant is the RNH. The person that bought that domain agrees to the terms and conditions that all RNHs agree to and accepts full responsibility for whatever happens on that domain. The registrar has RNH data. The registrar can disclose RNH data. The registrar can never know the intimate circumstances around why that particular RNH accepted responsibility for being a proxy for someone else. Next slide, please.

A lot of the discourse around PPSAI presumes that there is some party that is behind the RNH, someone who isn't the RNH, and that person is the person whose data is desired. Whether that person exists should be a threshold question to start with, since every domain is accompanied by a contract between the registrar and, say it with me now, the RNH. If a person exists who is not the RNH, there is no way for a registrar to know that, because, again, they have a contractual relationship with the RNH.

If you hear frustration in my voice, that is because I keep being told that this phantom party must exist and that I must know who they are so that I can disclose that data. But at the end of the day, the RNH is the culpable party. The registrar has RNH data. The registrar can provide RNH data upon a showing of appropriate due process based on their own policies, but they cannot provide information for an entity that doesn't exist or that they do not know exists.

GABRIEL ANDREWS: Hi, Reg, this is Gabe. So, I have a question, and this goes back to looking at the type of WHOIS data that we were looking to in Owen's example a second ago. But in particular, when you mentioned that you have potentially reseller operators that also operate as proxy services, and when they do, they are the RNH, is what I'm getting. Can you advise what information I should be seeing in the who is that tells me that versus the resellers that aren't operating as proxy services?

REG LEVY: Yeah, so when you pull up WHOIS, you will see either my privacy service or redacted for privacy, in which case the RNH data has been redacted. So, if there is a reseller who is the RNH, you will not see that information in the WHOIS because they are the RNH, and they are not using a privacy service. And you can send a request to disclose information behind WHOIS privacy, sorry, behind redacted for GDPR, and I will provide to you the information of the reseller, of the RNH.

GABRIEL ANDREWS: Following along then, just trying to get that then. So, fundamentally then, I would go to you as the registrar because there's nothing in there that points to the existing contractual relationship with the reseller because they're redacted. But you would be able to tell me who they are, and then I go to them secondarily to find out more information about their customer is the way that that flowchart would have to work. Yes?

REG LEVY: So, I would provide to you the RNH data, and you would go to the RNH with your complaint. Again, the RNH is fully liable for everything that happens on the domain. You can pursue legal and criminal process against the RNH.

GABRIEL ANDREWS: Copy. Okay. I think I follow that. So, essentially, you're just saying treat them like any other registrant at that point. Okay. Copy that.

PAUL MCGRADY: Thanks. And, Reg, I appreciate the detail of that. I also wonder, out in the real world, people not around this table, like some of us are struggling to understand it, but imagine someone that is not an ICANN person understanding that. I know that you get frustrated because everybody keeps asking you, like, who actually owns this domain name? Because they're not a phantom. Somebody has the beneficial interest in this. And so, I guess from my point of view, as I'm thinking about the end user.

Is there anything in the current policy that would require, that they were talking about implementing that would require any explanation that would give, let's not even say, the person around the kitchen table. Let's say some inexperienced lawyer in Kansas City trying to help his customer or his client. Is there anything in our policy that would require any guidance about how to actually understand the labyrinth of this? Because there's some-- Like I asked Owen, there's so many things that you have to know in order to know what you don't know in the way you've got that. You know what I mean?

And not being critical of the model. You know, I totally get it. But is there anything in the current policy that would help the requester to understand how that works? Or is that just a gap in the policy? Thanks.

REG LEVY: So, currently, Tucows redacts all registrant WHOIS data for GDPR privacy. So, you will see in the WHOIS, redacted for privacy. And you can come to me and ask what the RNH data is, and upon a showing of reasonable reason to have it, I'll give it to you. Registrants, per ICANN policy, are required to be allowed to publish their information in the WHOIS publicly. So, to remove the GDPR redaction. And we absolutely do that. Some of our resellers do that for-- Some of our reseller proxies will also do that so that they are publishing in the WHOIS that they are the registrant.

Again, I'm a little bit confused because when the lawyer from Kansas comes to me and asks for registrant data for a domain name because they want someone to pursue legal action against, that is what I give

them. Because where a reseller acts as proxy, they accept full culpability for anything that happens on that domain, just as every other registrant does. And so, your lawyer in Kansas can sue my reseller directly, and should, for whatever is happening on that domain.

PAUL MCGRADY: So, again, that requires the guy in Kansas City to know the difference between a registered name holder of the reseller versus the actual person somewhere that went and registered this domain name and is putting it to use, right? So, there's a knowledge gap there. And I'm not asking this question to be critical of Tucows. I'm being very, very clear.

The reason why I asked Owen what I asked him, the reason why I'm asking you what I asked you, is when all of this goes back to council, if there are gaps, that the original policy didn't cover, keeping in mind that the purpose of all this, which is this isn't for us, right? This is for people out there trying to figure out if a domain name is an abusive registration, how to address it, who to get to, right?

And if there is a gap, then we should identify those gaps to council because at some point we have to decide, what are we going to do with this thing, right? And so, is Swiss cheese good enough? If there's holes in it we don't know. And so, I'm not asking for purposes of being mean to Tucows anything like that. I'm just trying to find out, where are the gaps from a regular Joe point of view. Thanks.

REG LEVY: Yeah, and I'm not taking personal offense. However, when your lawyer in Kansas sues the registrant, it may be the case that they are a proxy registrant and they're going to say, “Whoa, whoa, whoa, don't sue me, sue this other person.” They may also say, “Bring it on. I accepted this responsibility.” They're the registered name holder. They have the responsibility.

JOTHAN FRAKES: Hi, Jothan Frakes again. Reg, I wanted to clarify, or at least understand better, when you had the direct conversation with Gabe Andrews, when you said you can come to me and where a domain is redacted for privacy and request it, and then I'll give it to you. Was that in the context of that being a law enforcement request or was that a general request for anyone? Thank you.

REG LEVY: It's anyone can make the request. Tucows has set up the tiered access compliance and operations portal, which we thought was very clever. It's taco. And you can submit a request through taco and answer the questions that the registrar stakeholder group recommended to answer in order to provide us with enough information to determine whether or not you should get access to that WHOIS data.

We will review that request, and then we will provide you with access in a secure manner to the registered name holder information. I will say for local law enforcement, it's actually a lot easier. You just have to say, “Yo, I'm local law enforcement, and I want information on a domain

name," and I give it to you. But foreign law enforcement and everyone else can make a case for it.

GABRIEL ANDREWS: I wonder if I could ask you the same question that I asked Owen in the context of what is escrow? Does anything change when you have resellers in play, especially if those resellers operate as proxies and might have customers underneath them or not and what would be passed?

REG LEVY: Yeah, we escrow registered name holder data. We escrow registrant data. That's the same data set. And if a registrant is using our privacy service, we also escrow the privacy service information.

GABRIEL ANDREWS: But just to clarify, then, if one of your resellers is also a proxy service, you are not escrowing any of their customer information onto ICANN, then, yes?

REG LEVY: Just to clarify, if one of our resellers is the registered name holder, we will escrow the registered name holder information.

MICHAEL PALAGE: Michael Pelage for the record. Question to both Reg and to Owen. Under NIS2 Article 28, the concept or definition of a contact administering the domain name is set forth. Both in Article 28 as well as in some of the guidance by the cooperation group. Can you opine or give insight on how your respective registrars define this term?

REG LEVY: I'm sorry. Do I care how resellers define what term?

MICHAEL PALAGE: No. My question is with regard to NIS2 Article 28 and the specific term contact administering the domain, which is distinct from the registrant name, registrant. And that was specified in Article 28 as well as in the guidance that the cooperation group came out with. They have expanded the definition. And I was just wondering if either of your registrars can give any insight on how they are going to define that term.

REG LEVY: So, in a lot of cases, a reseller will choose to put their information in the admin or the tech contact field, but they will still have their customer's information or other registrant data in the registrant field. So, an administrative contact may be available for some domains where that's appropriate.

DENNIS CHANG: I think Roger had a hand up and you've been waiting, but we we're out of time. So can you just go ahead in one minute.

ROGER CARNEY: Then I just wanted to try to hopefully fill a gap of a gap maybe that Paul mentioned. And the discussion has focused on resellers for some reason, but to Reg's point, I registered a name for a friend several months ago and it's under my name. So if someone comes and asks me about it, I'm technically liable, but I may tell you, hey this is his domain, seek him. So again, the conversation was there but it exists all along, this could be a lawyer this, could be anything along the chain. And to Paul's point, I don't think there's a gap there because I think that that just is a natural occurrence that happens. Thanks

DENNIS CHANG: Thanks everyone. I think that's the time. So let's stop the recording. And those of you who want to stay and talk some more, I'll be here for another half an hour.

[END OF TRANSCRIPTION]