
BARCELONA – ICANN GDD: PP IRT Working Meeting
Wednesday, October 24, 2018 – 13:30 to 15:00 CEST
ICANN63 | Barcelona, Spain

AMY BIVINS:

Hi, everyone, and welcome. I'm Amy Bivins from ICANN Org and this is the Privacy Proxy Service Provider Accreditation IRT Working Meeting. Welcome.

I, as most of you know, am managing the implementation of this accreditation program. So, today, we'll review the background of this project which most of you know. We'll go through it briefly. Then, we'll go into talking about the project status which is the big topic this week. And next steps.

If you have questions or comments throughout the session, go ahead and raise your hand. We're not going to wait until the end for Q&A. So, please, just go ahead. Come up to the mic and raise your hand.

For anyone who's not familiar with this project – we can go on to the next slide – the Privacy Proxy Accreditation Program is being implemented based on policy recommendations that were adopted by the GNSO Council and approved by the board in 2016. So, since the IRT was formed a couple of years ago, we've developed several documents, including a draft accreditation agreement, a draft policy document, a draft applicant guide, de-accreditation process, and a fees proposal.

So, the IRT has provided feedback on all of those materials and we've reached agreement on most of the items with a few exceptions. The first

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

one being the proposed fees. The IRT's feedback will be noted on the proposed fees when we proceed to public comment. There's also some disagreement between the registrar and public safety members of the IRT related to the law enforcement authority framework and the response time to emergency requests. So, that's another item that we're planning to flag in the call for public comments.

But the most significant open item at this stage, which you probably heard a lot about this week, is how to incorporate data privacy provisions into the accreditation program requirements. So, that's the bulk of what we're going to be discussing today. Next slide, thanks.

So, recently, ICANN presented a markup of the accreditation agreement to the IRT. The draft included several provisions that were intended to address data privacy, including a new data processing specification. The specification set out a framework for the processing and sharing of registration data and other personal data. It included a proposed legal basis and purpose for processing of this data, based on consent or a legitimate interest and other requirements related to data security, access to data by data subjects, etc.

We discussed this with the IRT and the IRT recommended that ICANN take a different approach. Some IRT members recommended that ICANN take out the data processing specification and simply allow privacy and proxy service providers to certify that they're compliant with relevant data protection laws. Generally, the feedback was that the specification was very focused on GDPR. And for privacy and proxy

service providers that aren't subject to GDPR, they shouldn't be subject to the specification. You can go to the next slide.

At this point, we've taken the feedback and we're trying to figure out how to proceed with it. Based on what we know, ICANN believes that we need some type of data processing provision in the agreement. So, at this point, we believe that there's still a significant amount of uncertainty around what the data processing provision should look like.

As a result, you've heard the messaging this week I'm sure, that ICANN is planning to slow down the work on this until we figure out these data processing issues.

We believe that the discussions in the EPDP may assist us in trying to figure out some of these issues. Also, potentially, the discussions with the European Data Protection Board. At this stage, we don't believe we should continue to push ahead to public comment until we have more certainty on those issues.

So, at this stage, we really want to hear from you about what you think about the status. If there are items that you believe that we should continue to work on and focus on at this point, we'd really like to hear your feedback.

At this point, we're continuing to monitor the work of the EPDP and the discussions with the European Data Protection Board. We're also planning to continue working on other items that aren't directly related

to the data privacy related discussions while we're looking to gain more certainty surrounding the data processing provisions in the agreement.

So, we've heard a lot of feedback about this this week. I don't know if any of you in the room have thoughts about this, but this would be a good forum to ask questions and provide any additional feedback. Sure, go ahead.

KATHY KLEIMAN: Kathy Kleiman. Amy, can we ask questions that aren't on the slides?

AMY BIVINS: Yes, absolutely.

KATHY KLEIMAN: Okay. First, thanks to everyone who is on this IRT. I know it's been a long time and long run. I was on the original PPSAI. My question has to do with cost. There's a lot of discussion in the hallways about what the cost for being certified as a proxy privacy provider will be and then what the pass-on cost will be to registrants.

And just so you know – I'll be candid. That why I'm asking, because I don't have the basis for knowing. But what I'm hearing in the hallways is it will be exorbitantly expensive and the very groups and individuals that we want who most deserve and need proxy privacy protection won't be able to afford it. That's what we're hearing in the hallways.

AMY BIVINS: Thank you for that feedback. There has been a significant amount of discussion related to the proposed fees for the program. There was a preliminary cost assessment done related to the cost of the program that informed the proposed fees. But we are very well aware that there are differing opinions among members of the community on this and we plan to flag this in the call for public comments. ICANN believes that there is a basis for the proposed fees and we believe they're related to the anticipated cost.

KATHY KLEIMAN: Any ballpark estimates?

AMY BIVINS: So, the proposed fee, the annual accreditation fee that's being proposed is \$4,000 a year. I don't know if that was ...

KATHY KLEIMAN: Can I ask anyone who's providing proxy privacy services, what that might mean in terms of costs passed on to the registrant?

ROGER: Hi, this is Roger. Actually, I think that most of the IRT disagreed with these fees and thought that they were way too high. Again, staff has their numbers that they think it has to be to support it. I think that's why the IRT left it as an open item for the public comments.

AMY BIVINS: And just to add on the fees topic, there's a requirement that fees be posted before they're considered by the board. So, this definitely is in the last discussion about fees. The opportunities during the public comment, we will take the community's feedback into account on that.

Do we have other questions? Anyone? This is a 90-minute session, but we do not have to take the whole 90 minutes. Roger?

ROGER: We do support the slower slowness of this direction. At this point, I don't think that we can realistically move on to public comment with so many open items outside of this group.

AMY BIVINS: Thanks, Roger. We'll take that feedback back. We are appreciative of that. I know we've had some questions this week about what items specifically we're waiting on. I think we'll probably be providing more information about that. If you look back at the proposed data processing specification that we had proposed for discussion with the IRT, there were data processing provisions related to the collection and retention of registration data. We received some comments this week that the EPDP is focused on registrars and registries and there's been some feedback that privacy proxy services are not the same. We were very well aware of that, but the data that's being collected and the potential uses for it are similar, so we do think that they're relevant but there could be further discussions about that, if you have additional feedback.

You guys are being really easy on me today. Steve's hand is raised. Steve, please go ahead.

STEVE METALITZ: Hi, this is Steve Metalitz. Can you hear me?

AMY BIVINS: Give us just a minute, Steve, while we figure out the issue with audio. Steve, can you keep talking, please?

STEVE METALITZ: Yeah. This is Steve.

UNIDENTIFIED MALE: Go ahead, Steve.

STEVE METALITZ: Hi, this is Steve Metalitz. Can you hear me?

AMY BIVINS: Yes.

STEVE METALITZ: Okay. After all that, I just have a very brief comment. We disagree with the decision to put this project on ice. It was already kind of in the deep freeze. I think this group has met three times since March, maybe four times. So, the slowing is already as past history. Now it's stopping. We

don't think the justifications that have been given are compelling. The EPDP does not have any remit in this area, so waiting for the EPDP is not a strong justification, waiting for the European Data Protection Board, waiting for [inaudible]. We're not going to get any useful guidance from them has been made manifestly clear.

So, we do object to this but I'm not going to belabor it here because the decision was not made here. We'll pursue other avenues to try to change this decision. Thank you.

AMY BIVINS:

Thank you, Steve, for that feedback. We have heard that feedback in several sessions this week and we're certainly ... I would expect that ICANN will likely be responding further to that and we'll be having further discussions about that. But the differing opinions on this topic are absolutely noted. Does anybody else have comments or questions?

UNIDENTIFIED FEMALE:

[inaudible]. I have a question about when some day the GDPR of fully implemented. I've already seen a lot of registrars that already full implemented regardless of the registrant's location. So, when the day comes with this [PP] still valid is useful at all? I don't see how this program can be still there when the GDPR is fully implemented.

KATHY KLEIMAN:

I can give you some reflections based on the original policy group, the original PDP. Would that be useful? The IRT may have some other thoughts.

So, obviously, proxy and privacy services is a service that costs money and provides protection and these was that certainly when the WHOIS or the RDS, whatever you want to call it, is no longer public, first the accuracy should go up and the willingness of people to put information into it will go up considerably.

But depending on how the GDPR – the EPDP – goes in terms of GDPR implementation, you may still need another layer of privacy for those who are human rights activists, those are who [inaudible], those who in their own countries could be shot or beheaded for being gay. There's an issue of what's criminal law in one country is not criminal in another country and in our global system. The registrant may not be protected based on the laws of where we are. You can tell I'm a free speech attorney. And there's great worry about this. But of course we'd never kill journalists. I just want to say that. No government would ever kill a journalist. That's the world we live in. Thanks.

UNIDENTIFIED FEMALE:

Yeah. But then the [inaudible] say that a gay person can be shot and killed, so the dictator, the country they wanted to know who the registrant is, right? So, do they, the government, have the legal authority to say, hey, you've got to release this data of this registrant? Still, they have the authority to do that, right?

KATHY KLEIMAN:

Actually, I appeal to those who are proxy and privacy service providers. The understanding of some was that there would be a higher level of scrutiny as some of these calls for ... Or that higher levels of protection might be provided as some of these calls for data. You might want to shut your mic off or we'll create an echo, I think, in the remote.

There's real concerns here. I wasn't being ironic. I've dealt with human rights activists who are doing something completely legal in the United States but they're expatriates of completely corrupt countries where they came from and their websites have been classified as treasonous.

So, if the names of ... If their names were associated with their organizations, their families who are still in those countries would be arrested.

So, there will be groups, individuals, organizations, and maybe businesses that are looking for that higher level of privacy and will seek them through the proxy privacy and be willing to pay for it and hope that there is more protection based on the national laws of where they're located and where the registrars and registries are located. But we're hypothesizing a future space.

We always talked about two levels of protection.

UNIDENTIFIED MALE:

I can see that the conflict or encroachment will be there when you're talking about RDAP, that level of access, [inaudible] access. So, if

[inaudible] certain officials government that they accredited to access the RDAP, then there will be a conflict there, right? Wouldn't it be?

UNIDENTIFIED MALE:

No, there wouldn't be. I think that's Kathy's point, actually, is potentially in the future, depending on what's decided. If they say, okay, law enforcement gets access to this amount of data, that's fine, but if they have privacy on it, they would still have to take another step.

RDAP is just a tool, but if the policy says, yes, law enforcement has access to this data set, that doesn't mean that there's not privacy on it and they still can't see it. So, they would still have to take another step.

AMY BIVINS:

Just to add to this a little bit, I think part of the disconnect or what may help with the understanding of this also is that law enforcement access will depend on where the privacy or proxy provider is.

For example, if you have someone that's engaging in some sort of speech that's free speech in the US but not somewhere else, if the law enforcement in this other jurisdiction is requesting the data from a US-based privacy proxy provider, the standard for access would be illegality under US law, not the other jurisdictions.

UNIDENTIFIED FEMALE:

Okay. So, maybe I missed the point of the RDAP, the data. I thought that a registrar is supposed to upload [inaudible] agree on [inaudible] instead of ... Just like right now the escrow [inaudible]. We are

supposed to upload all the registrant information. I'm sorry, I'm [Jocelyn] [inaudible] from New Jersey, United States. I was talking about the escrow. We have to upload all the data out of the escrow account, right? Then, I think we are required to upload all the real data registrant information, not the proxy of data in there.

So, with RDAP, eventually it will be required to upload [inaudible] data or just the proxy data.

ROGER:

Yeah. I think there's a difference here. RDAP doesn't do anything besides move data from one spot to another and there will be some access controls on it as well at some point later. But data escrow is completely different and isolated from any WHOIS. I mean, it's a different reason and it's there for a different reason. So, the escrow files, yes. The escrow files will probably I'm guessing still exist to some degree. But RDAP won't touch that, won't know about it, nothing, so that data is different. That data that RDAP will be getting access to will be the [inaudible] from the registries or the WHOIS databases from the registrars.

UNIDENTIFIED FEMALE:

Maybe I didn't make myself clear enough. I'm not talking about the escrow. I know the escrow data is different from the RDAP. I'm just asking the RDAP eventually that registrars will be required to have all the real data, not the proxy services data.

ROGER: No, that's not true. At least that's not ... Again, we don't know, right, today. The thought is, no, that would not be true. RDAP would pass back what the registrar has which would be the proxy data.

UNIDENTIFIED FEMALE: Okay.

AMY BIVINS: Alright. Any other questions or comments? Okay, great. In that case, we will follow-up with the IRT after this meeting to discuss more about status. Obviously, given all the feedback we've had this week about the status, we may have further discussions about what the process is and when we'll be meeting and what we'll be discussing, but we'll be following up with the group shortly after the meeting. Thanks, everyone.

UNIDENTIFIED MALE: Thank you.

[END OF TRANSCRIPTION]