

ANDREA GLANDON: Good morning, good afternoon and good evening to everyone. Welcome to the EURALO Webinar on GDPR on this Tuesday, 29th of May 2018 at 1800 UTC. Our presenters today are Michele Neylon, Oksana Prykhodko, Olivier Passek, Lucien Castex, Raoul Plommer and Teemu Ropponen. We will not be doing a roll call since this a webinar.

Please remember to state your name before speaking for transcription purposes. I kindly remind all participants on the phone bridge as well as on WebEx to please mute your speakers and microphones when not speaking. Thank you all for joining, I will now turn it over to EURALO Chair, Olivier Crepin-Leblond, you may begin.

OLIVER CREPIN-LEBLOND: Thank you very much, Andrea. Olivier Crepin-Leblond speaking. Today we've got an exciting webinar about GDPR post 25th of May 2018. You will have seen that your mailbox will have been filled with tons and tons of emails from different organizations, finding the last minute to tell you, "We need to be compliant, so we need to find out if you are okay with us having all sorts of information you."

It's a bit of a mess in a way because there doesn't appear to be a single way to cope with GDPR. We've heard that there is a lawsuit that's been launched by ICANN or court case that's been launched by ICANN against a registrar called EPAG but at the same time, this webinar is a follow up to our earlier webinars that we had where we spoke about the different points of view. First, we explained what the GDPR was about in an

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.

earlier webinar and then after that we had examples of how registrars and registries and end users were coping with this.

This call here is going to focus even more on our members. On how people will be -- are different At-Large structures and members are coping with this. We've got several different angles that we will be touching on. The one that we'll start with is one from Michele. He is an individual user but he also runs a registrar and he's got three different component parts he's going to talk to us about.

First, telling us a little bit about the latest developments on the temporary specifications for gTLD Registration Data. There are links in the agenda to all of the things that we're going to talk about, so there's a link to that. There's a link to the letters from the Congress, to US based registrars and registries. Then he'll be speaking a little bit about his registrar, Black Knight Internet Solutions is coping with the GDPR, what they've had to do to comply. Then he'll be explaining what the ICANN versus CPAC court case is. He has written a blog post about the case.

Then we'll have Oksana Prykhodko who'll be speaking to us about how the GDPR is affecting countries in Eastern Europe. She'll be sharing with us a little what's going on in Ukraine, in that matter.

Then we will not have Oliver Passak, who unfortunately is unable to attend tonight's webinar but I'll be reading through -- well, he has briefed me on what he was going to say and I'll be just explaining for five minutes, The Big Brother of Words, that digital courage, his At-Large structure runs every year.

Then we will have I believe Lucien Castex, I think dial out is waiting for him. I'll be sending the details to such shortly. Lucien is from the Internet Society French Chapter and he will be taking us through the E-Bastille Initiative. Trust the French to have a really cool, funky name for this.

Then afterwards we'll have Raoul Plommer who is from the Open Knowledge Finland and in assertion with the Internet Society Finland. They are doing a massive open online course on GDPR.

We'll have a discussion about all of these things afterwards. I think time will go pretty quickly. Let quickly move forward and have Michele Neylon to speak to us about his perspective and the latest version of ICANN's temporary specification. Michele, you have the floor and thank you for joining us.

MICHELE NEYLON:

Thanks Olivier. I hope everybody can hear me okay. Good evening everybody, I'm Michele from Black Night here. We are, for those of you who don't know me, we are a hosting provider and registrar based in Ireland and as Olivier pointed out, I'm also officially a individual user through the individual users At-Large structure. This entire thing with ICANN and GDPR has been interesting, which is probably the most diplomatic word I can use to describe it.

For those of who've been following this over the last few months, you probably know that at the meeting back in Abu Dhabi ICANN CEO said, "Okay, we're not going to take compliance actions. We're going to work

with the community, blah, blah.” And then people put in a number of different “models”.

Based on those models, ICANN eventually came up with a temporary specification, which is relatively long, reasonably detailed document that is based by large on ICANN’s interim model. It doesn’t match it 100%, there are a few areas of divergence but it kind of more or less follows that. The model is a bit of a weird beast because it supersedes the contractual requirements on registrars and registries, as well as superseding any consensus policy that might be impacted by it. It goes into a bunch of different things about the data that registrars and registries are meant to collect and process and a variety of other things.

Now, unfortunately because of the timing and GDPR as you probably came into full affect Friday last, May 25th. For registrars and registries, most of us had already been working, making changes to our processes and systems and everything else, in order to be as compliant as possible and by the deadline. The ICANN temporary was only released late on the 17th of May, so that’s basically less than a working week. The likelihood of all of us being able to make the changes necessary to be compliant with that was pretty much slim to none. Some registrars and registries aren’t even a 100% sure whether or not the temporary specification is full complaint with GDPR.

For those of you that are interested anyway, the temporary specification you can have a look at it, it goes through the bit and pieces. It tries to explain the purposes of the processing of the data and it provides a list of requirements which are applicable to registry

operators and registrars and then some are only applicable to registries and some that are applicable to registrars.

Also, around the same time ICANN announced that they had appointed another data escrow agent and this time one based in the European Union, which DNIC. Registrars can choose to use DNIC as their escrow provider. Several of us have started a process of moving to DNIC but it's my understanding that there's a bit of a delay since not all of the contracts that are required for that are ready as yet. That's what's been going on from the ICANN side.

Now, against the backdrop of course the political pressure, so those of you how may or may not be following all of this, the US Government and various other stakeholder groups, mainly intellectual property I suppose and possible others, strongly believe that making changes to public WHOIS will have a detrimental impact on the internet as we know it. They have been conducting a campaign of essentially lobbying politicians and pretty much anybody else who will give them the time of day.

If you look up the links in the agenda for this evenings webinar, there's a link there to letter from Congress to US registrars and registries and this where somebody in Congress essentially wrote to all the big US based registry operators and registrars, demanding that they explain exactly what they were going to be doing with WHOIS and to provide assurances that they wouldn't be making changes to it that would have a negative impact. That's kind of the backdrop to this.

From a political perspective it's pretty clear that the US Government via the Department of Commerce NTIA, David Redl & co, they have very very strong feelings about how public WHOIS should be handled and who should have access to it. These are -- ouch, that really could you please mute yourself, that really hurt. Those are views are at odds with the views held by most of the registrars, registries and pretty much ICANN as well.

On the registrar side, I can speak obviously a little bit about what my own registrar is doing. We have made changes to our public WHOIS. Just so we're clear about that, I'm referring is the WHOIS server that we operate. We're not making changes to the main registration data that we are collecting or processing or how we're handling that. It's more down to the public display. If you look at a WHOIS record for example a dot com. What we've done is we took the ICANN interim model and the eco model and we did a mash up between the two of those and pretty much all contact fields we have adapted for GDPR.

When you do a WHOIS lookup you'll no longer see my home address, for example, you will see redacted due to GDPR with the exception of you'll see the country and you will see the region. Obviously, the name servers, the create days, update days, registrar of record, WHOIS server, abuse contact for the registrar, all of those things are unchanged.

I'll send a link to a blog post I wrote about that to Olivier so he can put it on the notes for you. What we've done then is for the email addresses, we've replaced those with a webform. If you do a WHOIS lookup prompted to go to the webform and then on the webform at the moment it basically says, who are, what do you want kind of thing. We

will then send the message that you input into the form will be sent to the domain contact. They're under no obligation to reply to you. We are logging a bit of the information there because we're interested in getting some statistical data. I think that will be interesting for some kind of transparency report further down the road.

As I say, there's no way that we're trying to tell our clients, our registrants that they are going to be obliged to respond to any of these requests. That's essentially what we're doing around the ICANN WHOIS stuff. There's a variety of things within the ICANN spec that mostly don't have a massive impact. It's things like involving cases of UDRP or URS.

If the finer details of this haven't been fully worked so I don't know exactly how that will work. If WIPO or one of the others comes to us and say, "We received a case dealing with a domain that involves yourselves, can you give us the data?" In which case we will. But for other third parties who aren't [inaudible] law enforcement or who have not presented a court order to us, we're politely going to tell them to get lost, maybe not so politely, depends how they ask. That's our position at the moment based on the legal advice that we've taken.

Obviously, with respect to GDPR as I outlined the last time round, the GDPR stuff for us as a company is much, much broader than dealing with ICANN. In terms of what we were doing internally in the run up to last Friday, we're still working on it obviously. The ICANN slice was 5% of the workload because there's a lot more to it than that. Looking at all the data that we're collecting. Getting data processing agreements with

vendors. Having processing agreement available for clients, etcetera, etcetera, etcetera.

This entire thing that Olivier mentioned with all the crazy emails that a lot of companies have been sending around and our view was that a lot of those emails were completely unnecessary, that only companies that have been collecting and abusing contact details in the past really needed to go down that route. Where are as in our case, we sent a fairly simple email out to our entire customer base on Friday late morning Irish time, just outlining exactly what we do, where our policies and everything else were located and why we also feel that we're perfectly entitled to email our clients. If they want to get marketing stuff they have to update. That's our kind of position.

Friday came and went and the world did not come to an end. Our inboxes were still being assaulted with all the crazy GDPR emails. Then Friday evening ICANN announced that they were taking EPAG, a German registrar that has owned by two pals, they were taking them to court in Germany and that's where things got a little bit interesting. If you look at the ICANN announcement on the ICANN website they put out Friday night explaining what they were thinking and then if you look at the announcement from Two Pals that came out late last night or early this morning, which I covered in my blogged post that Olivier has linked to. You can see that there two quite different approaches on this.

If you go back and you have a look at all of the paperwork and all of the blog posts and the letters and more letters and legal opinions and everything else around ICANN and GDPR, what this case boils down to, is one single word, clarity. What ICANN is trying to or at least claiming

that they are trying to do, is to seek clarity around a particular aspect of this temporary specification. What they're trying to do, is to find out whether or not getting the registrars by extension the registries to collect and process all of the contact information for a secondary contact in the domain name registration data is legal under GDPR.

To put that more simply, when you register a domain name or if you do a WHOIS look up on a domain name, you have multiple contacts in the public WHOIS, even though now a days, obviously that's heavily redacted, so you have the registrant with the admin, you have the contact and you have the billing contact. Historically those contacts may have had some use and value but a lot of cases they're going to be identical or very, very close, no real difference. The rationale that EPAG in 2000 put forward is that, first off, they're very close or are identical in many cases.

Secondly, these are contacts that don't have any contractual relationship with the registrar and flowing from that, what value do you have, etcetera, etcetera. The ICANN view being, these are contractual obligations. We people to keep collecting and processing them, so we're going to test this in court.

I think that kind of covers pretty much everything. Did I leave anything out Olivier?

OLIVIER CREPIN-LEBLOND: Yeah, thank you very much Michele. No, that's fine. I think that's a good, well round points that you've made. We do have quite a tight agenda. I guess we can get any questions or comments and so on at the

end of the call when we'll open the discussion up but thank you for taking us through this. You might have not seen it but while you were speaking I did put in the chat the WHOIS details as taken from BlackKnight.com from WHOIS.BlackKnight.com and that shows the redaction for GDPR. Some discussion underneath that and I invite you take part in it. In the meantime, let's move on then to the next speaker and that's Oksana Prykhodko, who is from the European Media Platform. I'm not quite sure, I don't see her in the list participant but perhaps she's on the phone. Is Oksana with us?

OKSANA PRYKHODKO: Yes, Olivier, thank you very much. I am on telephone; can you hear me?

OLIVIER CREPIN-LEBLOND: Yes, we can hear you. Thank you very much. Oksana, you're going to provide us with some details of how things are perceived. How GDPR is perceived in Ukraine, so over to you.

OKSANA PRYKHODKO: Thank you very much. We have a lot of problems with GDPR.

OLIVIER CREPIN-LEBLOND: Have we lost Oksana? Might be dropped off.

ANDREA GLANDON: Yes, she just dropped, so we get her back momentarily.

OLIVIER CREPIN-LEBLOND: Okay. I guess whilst we try and get her back, then I can speak about the Big Brother Award. Oliver from Digitalcourage as I mentioned earlier couldn't make it to this call but what the Digitalcourage , his At-Large Structure, the Digitalcourage does, they're the co-organizers of an award called the Big Brother Award...yes, Oksana, sorry. I've moved on and then we'll come back to you.

OKSANA PRYKHODKO: Thank you very much. It's very much situation not only for Ukraine but also for our foreign guests and partners. So, I would like to stress out three points. The first one, on the governmental level, there is no understanding of GDPR importance for Ukraine at all. Ukraine is not EU member and even our EU Ukraine agreement association does not include the GDPR. This agreement was signed in 2014. This is why one year ago a lot of government associations thought that GDPR will not concern Ukraine at all.

We raised this issue in 2017 at our IZUA aid and representatives of our office ombudsman became responsible for data protection in Ukraine. After a lot of [inaudible] agreed only to come to listen but not to explain and answer questions. Then it was agreed that we need at least official translation from GDPR into Ukraine. It was a great progress for us that it was signed. Last year during our conference at Ukraine Parliament, Ukraine Internet Governance from a European perspective with participation [inaudible] from the European Parliament. It was agreed

to create group of experts the situation with GDPR to our EU Ukraine agreement one association, against huge progress.

The second problem is about institutional level. There is a lot of corporate and organizations which did a lot to get prepared for the GDPR but very few of them are really ready. As far as they know our CCTLD adopted some changes to WHOIS but actually they are not responsible for Ukraine WHOIS. Our organization, international nongovernment organization gets European media platform, is in an extremely difficult position. In 2010 they are registered as international NGOs, but last year the Ukrainian legislation [inaudible] was changed and there are no different rules now for international NGOs. We did not send letters for GDPR effectiveness to our members but we didn't ask for initial consultations of our ministry of justice.

The third point is about huge conflicts between data protection standards and access to information requirements in Ukraine. The ombudsman's which is responsible both for data protection and accessing information. Last year at EURODIG I met official Ukrainian representatives who refused to let you know your name and position because of data protection. I had to send official requests for information to the same ombudsman and to receive your name and position from another department. I think it would great discuss this issue at EURODIG Russia, as well as during IGFUA9 and [inaudible]. Thank you.

OLIVIER CREPIN-LEBLOND: Thank you very much, Oksana. That sounds like there's a lot going on and I look forward to hearing regarding this topic at [inaudible]. I hope that there is a session but that might be just a side session on this. Thanks for this. We now need to move back to Oliver Passek, Digitalcourage, and I'm just going to speak you briefly about these Big Brother Awards. That's basically an award that is given to a company or a piece of software or a process that affectively completely provides full privacy violation basically on various levels.

This year that was given over to a company that is listed here [inaudible] software for a piece a software that is used by the Federal Office of Migration and Refuges in Germany. The piece of software was named, making things very easy for the processing of migrants in Germany by having a single details and record of them because most of them do not have any legal documents and so on. They don't have passports, they don't have anything like this.

There was a software that was developed to try and make some sense into this and fortunately the software went way further than was originally anticipated and one of the concerns is that it's a building now a very, very large database of not only the names and details of those people but also their habits, it goes as far as what type of meal and food they were having.

So, they affectively in a country where the history has been that a very strong state has been met with a lot of catastrophes, speaking about the Nazi regime and the East German regime where the regime has mistreated their population based on information and data collection, this obviously would qualify for a Big Brother Award. That's the sort of

thing in light of GDPR that might need to be addressed whether this is GDPR complaint.

Digitalcourage asserts that is it probably not compliant and so has pulled the alarm on this one. That's one activity of our At-Large Structures that is perhaps not ICANN related directly but it certainly is an activity that's related to GDPR.

Now, I am hoping that, yes, I'm told that Lucien Castex has joined us from the French Chapter of the Internet Society. The French have looked at a totally different angle, which is to have an E-Bastille initiative and that's quite an exciting name. I'm looking forward to hear. There's a link in the agenda of course to the E-Bastille, it's all in French, so we're looking forward to hearing from Lucien as to what this entices and what this means. Lucien, you have the floor.

LUCIEN CASTEX:

Hello everyone. Sorry for not joining you earlier. I'm on the Organizing Committee of France IGF, so I'm a bit late. I wanted to summarize the main initiatives that we are doing in France around the GDPR. Obviously, the E-Bastille initiative and related events. Quickly, ISOC France organized [inaudible] European Civil Society Workshop on the compensation of data protection asked with the main aim to look at national implementation of Article 80 of the GDPR and basically to look at possibilities for collective address, to arm due to violation of data protection rights.

Very quickly the plan was to discuss methods to evaluate the amount of financial compensation that you could obtain in court in French and

other European countries. We organized a workshop and we had quite a few participants. Obviously, ISOC France participated but also NGOs in France like La Quadrature du Net, which is a civil society organization which is attacking with a class action mechanism Google, Amazon, Facebook and I forgot one probably, Microsoft before European courts.

We had also [inaudible] foundation from Poland, The European Bureau for Consumers and representatives from Academia in France, in Netherland and the UK and lawyers. That was a quite a good first steps to understand compensation and try to have a solid framework on Article 80 of the GDPR. Now under the E-Bastille initiative basically aims at writing public awareness on data protection. It's an initiative based on Article 80 the GDPR but also on the French implementation of the law, which [inaudible] process in France and is today not enacted because the constitution council needs still to address it.

Basically, the law in France follows also for compensation, which is not the case in every European country. The point of the E-Bastille initiative is to try raising awareness of the public and try to do some education and try to do it basically using the collective action mechanism while to - - let me rephrase it, basically the collective action mechanism aims at raising awareness of big players and citizens to try and empowering them on the personal data, it's basically main aim. We are using what we call E- doléance, which are basically a questionnaire that people can answer stating what they found to be problematic with the use of their personal data and with such E- doléance we are trying to make cases of data protection relations and to do a bit of legal analysis on that.

Also, to address directly big players and companies relating personal data in use in the frame of the GDPR and to make basically the problem stop or else we will use collective action mechanism and the ability to obviously to make it compensated of French law, that is the main aim of the action. Last quick point, I hope you can hear me well. Last quick point, we have another project on the question basically on terms of services.

As you all know there is a few problems with consents and terms of services since nobody really reads them completely or reads them at all and we are a project in France to try simplify term of services to make them readable in plain English basically. We are linking it to GDPR, it's a problematical run consent, can you really consent when you don't read and when basically you just click to get rid of it and use the service, which is quite a bit of a problem when you see Article 29 guidelines on consent and even when you try when you rate the proposal of a e privacy regulation on such matters. Very shortly that's what we do in France at ISOC.

OLIVIER CREPIN-LEBLOND: Okay, thank you very much, Lucien. That's a very interesting angle with the collection action and certainly all of the use of the net and so on in order to do this. Very interesting indeed. I hope you can stay with because there will be questions afterwards. But next we have to go quick swiftly to Raoul Plommer who is coming from the Open Knowledge Finland Internet Society Finland. He is going to tell us about a massive open online course on GDPR. That was something that was quite needed. Let's have Raoul.

RAOUL PLOMMER: Hello everyone. I'll try and tell you a little bit about the citizens view of how the GDPR has affected them. The digital rights are basically an online for learning about GDPR but we wanted to have the kind of compelling examples of how to exercise those rights. We've actually started going the road of actually trying it for ourselves and making subjects access request to different companies. Someone's mic is left on.

OLIVIE CREPIN-LEBLOND: Hopefully however is doing this is going to go to the next slide.

RAOUL PLOMMER: Okay, that's it. Here's basically the project timeline. We started off end of January and we've had three different workshops now of which the last one was the biggest one on Saturday. Unfortunately, the attendance was a little taxed by a really wonderful sunshine here in Finland which is rare but we still managed to have 22 participants who were interested in data protection.

Over the summer I got such exciting and this last workshop that we will have one more subject access request workshop in July, that's not really on the timeline there but I'll be making some requests with other people in mid-July. Then there's my data conference where the online course will have a session on it's on and a workshop. Still gathering content and trying to come up more compelling examples of how the GDPR is exercised and in an easy was as well. Then during autumn and

early winter we'll start to have online lectures, probably going to a few different universities to present and our finding.

These are basically the deliverables of the [inaudible], we'll have a few live lectures and it's basically we're creating a nest of new digital rights modules for people to learn about and we got the finance for the first one which is the GDPR and my data modules from internet society and the Finnish Foreign Ministry. We're using some of that money to purchase a platform license and have some funky video and graphic design on it. We got one of the videos done during this last workshop with Olivier [inaudible] giving a keynote there.

The goals are basically to increase awareness on GDPR and my data as well as other digital rights. Like I said, it's going to be a net for new additional modules in the future. This is just basically I'm giving you an idea of what kind of companies hold your data, what kind of companies that data can also be requested from. That basically goes for all the companies but these are really the ones that we've made some requests to, which we've found that these are the companies find most interesting to know what data do they have of them.

We're still actually exercising only the right to access rights so far, which we thought would be sort of the easiest right to exercise but we've had difficulties in even exercising that. We haven't started testing data portability from the citizens perspective but we'll work on those in the later workshops as well.

We also thought of making a small questionnaire to companies, maybe like a cover letter with this request, asking the companies how would

you like this data to be requested in, like what would be the wording for such request, because I think both sides can benefit from the fact that the data requested understandable and really we'd also want to find out how granular can those requests be, can you ask just for a specific thing or would you always get a huge pile of data of you, maybe even in raw format. We are still finding out.

This is just a couple pictures from the workshop. Basically, in this workshop we found out that it is really difficult to find the contact details of the data protection officers, not in all cases but in a lot of cases. One particular one I've captured in this presentation, which was Pinterest. I really found that one to be hard for anyone trying to get their data off them. There's lots of different kinds of procedures for identifying the data subject, it varies from portholes and secure email to sending a picture of your passport over clear text email.

It's like these companies have some processes from bad to worse. There are some that are really good, you can actually go and just download your data but even those, you can't really be absolutely sure that you're getting all of it, like in the case of Tinder, Oliver told us in his keynote speech. A lot of companies don't seem to be GDPR compliant. There was a case, we made the data request and one of the cases he was asking for a customer loyalty card in a retail store and he could actually see his ex-wife's purchases and they'd been divorced for a few years already and he could still see the most recent purchases on hers, so I don't think that's actually GDPR compliant. I think we'd actually be talking about a data breach there.

There was also with the same company, you could also identify yourself without a pin number, you just give them the credit card number but we'll dig into details of those before the next workshop. Here's an example of Pinterest. We were trying to exercise our right to access, try to find out how do we get to download data or get the data that's about us and if you go to the page where they have their privacy policy you see a couple of links there. It says basically to exercise these options, please contact us and it has a link to a place where you're supposed to be able to contact them about exercising these rights.

One of them is access the information we hold about you, we'll usually share this with you within 30 days of you asking us for it. We click on the contact us, next slide we see what actually appears. It's a page like this, asks still need help, send us a note, okay, what do you need help with. You select and there's five choices of which none of really tell you where to make your data request. After trying all these out, it's actually you can on the next slide it's reporting something was right answer there. These are the ones that you get after.

Basically, there's still nothing about having your data request done and in fact privacy is put together with harassment which I can sort of understand but that's not really anything to do with having your data request. Then you choose the harassment or privacy, it gives you a little more tips about it but that doesn't help me, this is really talking about completely different issue than having my data from their service. Next slide you see I need help. Then when you actually push that button that I still need help you finally get a form where you can explain your issue.

One of the things that actually struck me there was that it was only for customers of Pinterest although I imagine they have a lot of data of people, even people who aren't their customers, say in the form IP address. That was really quite difficult and I still haven't heard any response from them, from Pinterest after three days. It's really not obvious. One does not simply make a data request, it's harder than it should be.

This is what happened in our workshop. We made dozens of subject access request to different companies, about half of them Finish, have of the International. We're recording the process of each subject access request, so we actually know the process for each individual company of how to get that data all the way to you. There's issues like process for identification and the contact details of the data protection officer of the company.

We also got a nice video of the key notes by Olivier who told us more about the business perspective of the other side who actually get's these requests. These videos are still being edited. We also have those 22 participants who have a lot better idea of how to make a data request and are in the process of getting theirs. I think we're looking into some really interesting results and I think might even be in the topic in the coming week in the national newspaper. That's me, you can show the next slide of the happy people who did get out there, even to the sunshine. Thank you.

OLIVIER CREPIN-LEBLOND: Thanks very much, Raoul. I guess we have time for about 10 minutes of questions and comments. Let's open the floor for a discussion. In order to speak you may put your hand up in the chat or if you are not on the WebEx them please say your name and then I will provide you with -- we'll I'll put you in the cue. While people are gathering their thoughts and these are really interesting points of view that we have here. I have a couple of questions for various people.

I was going to ask Lucien regarding E-Bastille, is there any part that actually relates to domain name registrations in WHOIS? Is there any of this, I mean will it cover that as well? Is Lucien Castex still there? Okay, we might have lost him. Okay, I'm unphased. I've got a question then for Raoul as well. Two questions actually, the first one is, who will be able to use this [inaudible]; is it for public use? And who are actually your target use for this?

RAOUL PLOMMER: I think the biggest challenge in making this [inaudible] case is for it to try to reach as many people as possible and to make it interesting for as many as possible. The GDPR as exciting as it is, it's not really something people might find interesting to spend a few hours to learn about it. We really wanted to -- I've come up with one compelling example of exercising your rights and under the GDPR and that would be using the right to be forgotten with telemarketing companies. Everybody can relate to the fact that they want these marketing phone calls at whatever time during the day. That's the kind of angle we'd want to give them, instant gratification for bothering to learn their rights or exercising their rights.

OLIVIER CREPIN-LEBLOND: Thanks for this. The second question is, when was the test with Pinterest done? Was that a recent thing or was that at the beginning of the year?

PAOUL PLOMMER: I actually did that just before linking that presentation tonight. I just repeated tonight but it was already done during the workshop.

OLIVIER CREPIN-LEBLOND: Interesting, very interesting. Thank you, very helpful. There was some discussion in the chat regarding the redaction of GDPR records. I wonder if Michele wanted to say a few words about this?

MICHELE NEYLON: Sure. I don't know what you want me to say. We're redacting WHOIS records based on GDPR, based on the ECO Models, based on the ICANN Interim Model, based on the ICANN specification. We are a European company. We are bound by GDPR. Article 29 and multiple other data protection authorities of experts have said on multiple times over the last 15 years that there massive issues with public WHOIS. If you don't like how our public WHOIS, well don't use as a registrar.

OLIVIER CREPIN-LEBLOND: Thanks for this, Michele. There was a question, I recall in fact a discussion going on about the actual collection of the data. I guess that

the overall recommendations from ICANN have made a decision on that, regarding the actual collection of the data.

MICHELE NEYLON:

Okay, so this is where there's a bit of divergence of opinion. From the perspective of I think a lot of registrar and registries collecting data about a domain name is registered for we would see that as being not an issue. There's a multitude of reasons why having that information is important and if you want to look at in terms of GDPR and the legalities, again, I think a lot of us don't see that as being a problem.

The case between ICANN and EPAG, isn't about the registrant data, it's about the other contacts. If you want to look at this in a slightly different context, if you have a look at the WHOIS data that is collected and displayed by a lot of the ccTLD's, you find that many cases the only contact that they actually care about is the registrant, they don't really care about other contacts. From our perspective as a registrar, we're not overly concerned by this, for the simple reason in most cases the data that we're populating there, in those fields is going to be the same as the data used --

OLIVIER CREPIN-LEBLOND:

Have we lost Michele suddenly?

MICHELE NEYLON:

No, I'm here.

OLIVIER CREPIN-LEBLOND: Okay, keep on speaking.

MICHELE NEYLON: Somebody else was making lots of interesting noises. The big difference now in the current situation, collection and processing of domain registration data hasn't changed that much, what has changed is how the data is being displayed to the public. If you look the public WHOIS output for domain name registered through ourselves or one of our competitors in a gTLD, you're not going to get back as much information from a public WHOIS look up as you would have done prior to last week but we still have the information, we're just not sharing it with you.

OLIVIER CREPIN-LEBLOND: Thanks for this Michele. Lutz Donnerhacke, you have your hand up.

LUTZ DONNERHACKE: Hello everybody. I have to intervene the issue that nobody's looking at any contact data as part of the registrant. I'm very old man here, so I'm looking at technical context because for me WHOIS is the primal tool to debug issues that contact network issues. I do need the technical people there and I'm very happy to help them in the database so I can look up another way, then contact [inaudible] over the broad connection, that the first point.

Second point, collecting data and do not displaying is plain illegal. It's a violation of every rule and privacy, so we can't do this. What we can do is, using a WHOIS approach, as we have in other IANA WHOIS server, if you ask the IANA WHOIS server, who is this domain we have a contact

with the following registries, ask them and you get the contact data from the registry and though you can step by step go deeper and narrower to the selling point of the resource.

My question is, if we had such [inaudible] would it help to point down the contract up to the final point of the registrar who is covered by local law and maybe do not distribute the data to anybody else but display it according to local law, that would be sufficient by my personal point. Thanks.

OLIVIER CREPIN-LEBLOND: Thank you for this, Lutz. Michele, is this something that's workable?

MICHELE NEYLON: Short answer, no. First off, collection of data without displaying it is completely legal and I don't know why you would think it is not legal, it is a 100% legal. We collect and process quite a card of details from our clients every single day. In fact, it would be illegal for us to display that, so I don't where that's coming from. Secondly, with respect to being able to contact people, you can still do that in public WHOIS, just not giving you the email address.

Most registrars are using a web form in the public WHOIS or they're using some kind of email forwarder. But I wouldn't expect my mother for example, to understand if you sent her something about some technical issue with her domain, you're better off addressing those kinds of technical queries either to the hosting company or to the registrar. The thick WHOIS argument, fine.

The problem is if you publish the information under local law, the only way I could do that legally would be if I kept a physical register in my office and allowed you to come to the office to examine it. If I put it on the internet in any shape or form, then it's being transferred abroad, so I don't see how that would work.

OLIVIER CREPIN-LEBLOND: Thanks. Go ahead, Lutz.

LUTZ DONNERHACKE: Collecting private data, it's illegal as long as do not have a valid reason to do so. You do not process this data, you only keep it for other persons, for other people, for instance for law enforcement but offering this data at a different legal zone, especially in the USA or Germany, contact data from Germany to USA, law enforcement people have access to the data there, it's illegal simply because they have to use the process to capture data from another country. You are violating all the mechanisms which are in place in order to get data from different country.

They have also a law to fulfill which data needs to be given away and which needs to be protected [inaudible] bypass all this by giving the data out of the legal zone you are collecting the data in. It's not possible to say simply because we can collect other data or other purposes we are allowed to collect every day for any purpose and we do not tell you, sorry, that's not an argument.

The other point, there is a problem with my mother. I have a lot of customers which have a lot of problems, technical issues, of course they have somebody they can contact but if they want to process the resource on the internet or something else, for instance they have a car in the traffic system, they are responsible for it, they can't say, "I do not have any idea how this works, please stop it." If I do this, they have no right to use the result and that's not what we want to do. The people who own resources have responsibility to deal with it, sorry.

OLIVIER CREPIN-LEBLOND:

Okay, thanks for this vigorous intervention Lutz. I think that we probably would need another half an hour to get to the depth of those discussions. I just wanted to add one small thing. I did quote on the chat the Black Knights email WHOIS records and actually doesn't show the registrar abuse contact email address, that's because I did a screen capture and actually it is on the actual screen itself.

There is an abuse contact email that one can contact. Which I gather would server as a technical contact as such if there is a problem with that domain name and I would imagine that this get's read very regularly. I note that we are eight minutes past the top of the hour and there are no other people in the cue for questions. First, I wanted to thank all of our panelists for having spent the time to prepare for this presentation and to share some of their knowledge and wisdom and their points of view and projects and so on. I hope it was an interesting call for everyone.

This call is of course recorded, so we'll be making some announcements on the EURALO list after this call for people were not able to make it, to be able to listen to this call. The next steps after this, well for the time being, on the GDPR we don't have a forth coming webinar as such. Obviously, this is likely to be a topic that will remain in our cross wires for quite some time and definitely in the forthcoming meeting taking place in Panama. Of course, very soon next week at the EURODIG.

I invite you all to continue the discussion on the mailing list and if there is an interest another webinar in the near or far future, depending on what happens with ICANN versus EPAG, depending on whether there are other cases, then we're absolutely open to have further webinars and to have further updates, even on the Big Brother Awards, what's going on in Ukraine, what's going in Finland and other places as well. With this, I'd like thank our staff for tonight and everyone else and wish you a very good evening. For those people coming from other regions, very good morning, afternoon and night. Thank you and have a good time. Bye-bye.

ANDREA GLANDON:

Thank you. Today's webinar has adjourned. Please remember to disconnect all lines and have a wonderful rest of your day.

[END OF TRANSCRIPTION]