ABU DHABI – Cross Community Session: General Data Protection Regulation (GDPR) Implications for ICANN #
Thursday, November 2, 2017 – 10:30 to 12:00 GST
ICANN60 | Abu Dhabi, United Arab Emirates

THOMAS RICKERT: Good morning. This is the two-minute warning. I'd like to ask all the panelists for the GDPR session to come to the podium and take their seats.

Is Stephanie Perrin in the room? Stephanie, if you're in the room, I'd appreciate if you came up to the podium.

Let me ask again, is Stephanie Perrin in the room? Stephanie, if you are, I'd like to kindly invite you to the podium. So can you please all be seated? We're going to start the session. So good morning to all of you. Good morning, good afternoon, good evening to all the remote participants, wherever you are. My name is Thomas Rickert. I'm with ECO, an Internet industry association, and I've been asked to chair this GDPR-related session, which I gladly accepted. Now, let me first of all, introduce you to the panel. To my right we have Susan Kawaguchi. She's here as one of the chairs of the RDS PDP working group. Then we have Laureen Kapin from the FTC. She is here in her capacity as chair of the public safety working group in the GAC. Then we have Nick Wenban-Smith. He is with Nominet, and he's the general counsel there. Kevin Kreuser, he

is assistant general council with GoDaddy. Becky Burr from the ICANN board. Goran Marby, CEO of ICANN. And then we have Mr. Ralf Sauer who is participating remotely from the European Commission DG Justice. So let's do a little sound check with Ralf. Ralf, are you there?

RALF SAUER: Yes. I can hear you perfectly.

THOMAS RICKERT: That is awesome. The wonders of modern technology.

RALF SAUER: Indeed.

THOMAS RICKERT: Now, the panelists will have an opportunity to add information about their positions and what they're doing as they get the opportunity to speak for the first time. But let me now try to put this into context a little bit. The GDPR topic has kept everyone busy for a while. I think everyone knows by now what the GDPR acronym means which is the General Data Protection Regulation. And I would like to just to give you a little bit of

background information on GDPR so that you can put things in context.

Now, GDPR is going to be fully in force as of May 25th, 2018. And that is exactly two years after it has been -- after it has entered into force. So there's a distinction that it enters into force and then it applies. So it will apply as -- as of May 2018. But, of course, it is not a new act of law.

Then what you should know is that this is a directive -- this is not a directive. It is a regulation and therefore, it applies immediately. So there's no translation into national laws required.

Now, you might ask yourself as a non-European party, why GDPR could affect you, and, in fact, it will. If you have customers, if you process or otherwise collect the data of European data subjects, you need to be compliant unless such processing is just occasional. So if you as a contracted party have a customer base in one of the European countries or if you treat -- if you deal with data of European citizens, then that law would be applicable to you. And you might say, well, why should I bother? I'm sitting in some other country. But actually there is a requirement for you to appoint a representative in the EU, and if you fail to appoint a representative, then that in itself will make

you subject to fines up to 10 million Euros or 2% of the global annual turnover.

Then, a lot of talk is about WHOIS and GDPR compliance. And in fact, we're primarily discussing WHOIS today and the issues for the WHOIS system. But the issue is far broader. So GDPR is not only about WHOIS, it is about the collection and processing of data between resellers accredited registrars, registries, ICANN plays a role in there because they prescribe what needs to be collected in the WHOIS specification and they actually enforce breaches of the WHOIS specification. Then we have more players, the EBERO, the emergency back-end operator, and data escrow, who can get access or do actually get access to data. So one needs to look at the system holistically and come up with compliance models holistically in order for the parties not to be at the risk of being fined.

One other thing, because I guess that's a common misunderstanding, is that even if you are entitled to collect certain data elements, that doesn't automatically mean that you can publicize them for the general public. So every -- every step from collection to deletion of data elements needs to be carefully analyzed.

Now, for contracted parties that poses a specific challenge because if they want to be compliant, that might mean for them

that they can't continue to operate WHOIS services as we see them today. So they will be at the risk of either risking breach notices from ICANN or being sanctioned by Data Protection Authorities. And also, on the other side of the spectrum, we see law enforcement that is potentially hampered and IP lawyers that are being hampered of doing their investigations if WHOIS does not appear publicly as it does today.

So there's a predicament, there's limited time to fix things, and what we're trying to achieve today is have a good and meaningful discussion about ways forward. What you see on the screen here is something that we're going to get to after we've tried to understand the pressure points for the various parts of the ICANN community. And that is to find a way forward on how we can serve the needs of the various players in the game.

So what you see on the left-hand side is -- and we'll get back to that in a moment -- is the current status quo. But then as we might see part of WHOIS go dark, we need to find a way for ICANN to interplay with the contracted parties so ICANN does not sanction and issue breach -- breach notices to the contracted parties. So during that phase -- and there has been some common understanding in the preparation for this session -- we will need to treat this primarily as a contractual compliance issue. But as you know, a lot of work has been going

on in ICANN on WHOIS and the consequences thereof, so there is a more overarching policy discussion that needs to take place where the whole community needs to chime in. So we need to find a way to deal with this in the interim period, and then for the long run we need policy work to be done and the community to come together on that.

Now, before I open it up for the panelists to talk about the pressure points, let me set the scene by mentioning one quote from Goran's predecessor, Fadi Chehade, and I'm sure that some of you will remember this. When he did his first speech as ICANN CEO he said, there are two issues in the world that seem to be -- that obviously can't seem to be resolved and that's the Palestinian conflict and WHOIS. So I'm not sure whether I would have picked that example, but I think it illustrates quite nicely that WHOIS has been an ongoing subject of debate.

Okay. So now, we're going to have three sections during this discussion. We're going to hear about the pressure points of the various parties that are represented at this table, and I'd like to take the opportunity to welcome Stephanie Perrin as well who will speak eloquently to the interest of data subjects, i.e., users whose data might be published in WHOIS. And then we're going to talk about a way forward. And this is why you see this chart on the screen, so that you can already take a look at it. And after

roughly half of the session, we will open it up for questions from the plenary and from the remote participants and hopefully have a good discussion. Okay. So let me start with Nick to my left. And Nick, can you please make a relatively short statement about the challenges that GDPR will pose on registries.

NICK WENBAN-SMITH: Thank you, Thomas. Good morning, everybody. Thank you, I think, for the opportunity to speak today. I'm a member of the registry stakeholder group. However, I should make it clear that I'm not speaking on their behalf. I'm speaking here in a personal capacity.

So in a former life I obviously must have done a very terrible thing because today I'm the data protection officer for a number of top-level domains which are based in the European Union. And I have to tell you this is not a role for people who like to be liked. This is not a popularity contest.

So from my background, as an initially corporate and intellectual property lawyer, I've had to go on a bit of a journey with regards EU data protection lawyer, and I can sort of see that mirroring in the conversations that ICANN is having today because ICANN contracted parties are essentially dealing with rules and schedules which are very detailed and specific and

prescriptive about what you have to do and that totally contrasts with the principles-based regulatory system of EU data protection law. And I think that this is a very important point to understand at the outset, that you're talking about a principles-based regulation system. What you mean is, you have statements of law which are fairly vague and general, in essence. So when it comes to, say, the accuracy of personal data, the text of the GDPR regulation, for example, it doesn't require absolute accuracy, or a prescriptive sort of format. But it speaks of having to take reasonable steps to make sure that inaccurate data is corrected. And I think anybody who's ever asked a lawyer what the word "reasonable" means in a particular context knows that it comes down to judgment, balancing competing demands. Depending on the factual situation, there are a range of possible outcomes which are all possibly correct but different, and similarly to about fair processing of data that inherently, in my view, includes an element of subjectivity. So what is fair processing in one person's eyes is unfair processing in another's. And when it comes to then compliance of this, because it is all enforced by Data Protection Authorities in the jurisdictions within the European Union, what you have to do is you have to explain to the regulator who's threatening compliance action following various complaints about your organization's thought processes, your documented policies, your training, and it's a

sort of cultural compliance thing. And they're more interested in not what went wrong but what you're going to do to stop it from happening again in the future, if something has gone wrong.

The second point about the principles-based regulation is that because they're overarching principles, it's basically impossible to avoid them. It's very hard to have a work-around. You basically have to comply. It's very difficult to find any way in which you cannot escape the consequences. And I suppose finally around the principles-based regulation is because you're talking about technology and societal change, data subject expectations, these things are not static. They vary over time. What might have been compliant 20 years ago, 10 years ago, may not, in today's situation, be compliant anymore. So we've already seen this week, for example, the Dutch Data Protection Authorities have gone on public record that unlimited publication of WHOIS data already violates existing privacy laws in the EU and will be in violation of the GDPR. And that's interesting, because GDPR principles are not actually new. In the EU we've had to live with a similar sort of regulatory regime for at least the last few decades. And I suppose I totally understand the difficulty that the communities are facing because people are already saying that this is the biggest change in data protection law in the generation, but then if you

actually listen to speeches by the information commissioners in the different jurisdictions, they're all very much saying, ah, it's an evolution here, not revolution. All the principles are basically the same. So I can understand why people find it sort of difficult and seems there's a dichotomy being put here, and it's not very clear to see what exactly people mean.

So we had, at the moment, the 1995 directive. That led to national implementation up through national laws. There's a patchwork quilt. And the GDPR is going to attempt to harmonize that. Whether it does actually lead to harmonization is another very difficult question. So we're based in the U.K. Whether we will be bound by the Dutch Data Protection Authority's rulings going forward is not that clear to me. And I'm not entirely convinced that there will be the level of harmonization within the EU that people are expecting.

One of the big changes, I think Thomas alluded to it already, is the level of fines for breaches of GDPR, 20 million Euros or 4% of global turnover. And I think the way that I would characterize the change brought in by GDPR is that organizations who consider themselves to be following best practices on an almost optional voluntary basis will find that actually that is becoming much more concrete in terms of law. But I would urge communities to not get too hung up over the level of fines

because I think that from a -- a registry operator perspective what I'm much more concerned about is the -- the reputational aspect of being non-compliant because data is our core business and we absolutely want our best practices and we believe that we should do. So then to find ourselves in a situation where we're faced with two difficult choices, to comply with our legal obligations or to take our chances with ICANN compliance, and I think, speaking for the majority of registry operators, we'd choose the first one and we take our chances with ICANN compliance going forwards.

And although we're talking today primarily about WHOIS and publication, GDPR applies, it's worth saying for the record, across the whole of your business activities. That includes, you know, the security standards you apply to data, your HR processes and systems, and a whole bunch of other things for anybody who's operating within the EU as a business, and we all are.

And I just wanted to sort of end on a -- a sort of a positive note which is, there are -- there are many existing WHOIS models amongst the ccTLDs and we have managed to comply. I don't know of any EU ccTLD who has been threatened with enforcement action, and many of us have excellent relationships with our law enforcement and legal rights protection

communities, many of my European colleagues in the room today, there are plenty of other very good examples. And I'll just leave by saying the U.K. WHOIS, for example, we already and have, for the past decade at least, published less data in our WHOIS, and we haven't had any problems with that. And specifically, for individuals, we've always provided non-trading individuals with a free opt-out from having their address and contact information published in the WHOIS and it works pretty fine. So on the one hand, yes, it's very serious. We must work together to fix this. But on the other hand, there are solutions, and it's not a sort of an Armageddon. Thanks.

THOMAS RICKERT: Thanks for making Armageddon the last word of your statement. That's very encouraging. Thanks very much, Nick. Let's now move to registrars. So Kevin, shed some light on the predicaments for the registrars.

KEVIN KREUSER: Yeah. So I think Nick did a good kind of overview, so I'm going to not focus on how we got here and instead just highlight a couple of things. And one is, he pointed out that WHOIS has had a conflict with privacy law for a long time. GDPR is -- and the fines and penalties I think are what is motivating the community, for

better or worse, to finally focus on this issue. The issues for registrars, I think, is fairly obvious, and we're the ones who, you know, are kind of the point of collection for our customers. And the issue with collection, transfer, and publication under privacy laws around the world is something that, you know, we're fortunate to finally be addressing. What we do with it is an entirely other thing.

But I want to focus -- you mentioned previous to this, talking about pressure points, and for us, at this -- this time, you know, I think it's accountability and timing and, you know, the ball has been dropped here. And nobody's, you know, rushing to pick it up. And for us, it's very frustrating because while we very much respect the -- the value of WHOIS and what it does for the security and stability of the Internet, if you take away the contractual obligations that are on registrars and the compliance enforcement behind that, you know, what becomes of WHOIS? And what does that say about who's the controller and who should be picking up responsibility here?

That said, you know, as registrars we are working on looking at solutions because we want to be good, responsible members of the community and do what's right as far as WHOIS and the stability and security is concerned. But we need to get beyond opinions of law firms that are speaking to things of consent and

legitimate interests and necessity of contract and start exploring viable solutions because WHOIS, as it exists today, is very unlikely something that's compliant under GDPR or even the directive. There's -- I don't think that there's not a workable framework that exists. There are mechanisms in GDPR that can be exploited and leveraged and WHOIS can mold to that just as much as we can mold GDPR to what we -- what we want to do, but we need others to help and cooperate in driving that effort so that we can come up with some solution that's viable. But unfortunately we have seven months, roughly, to go, and as we all know how fast this community works, that's scary. And so, you know, this kind of accountability timing issue, and then also the uncertainty because we can come up with whatever we want and the unless DPAs say, you're good to go, we have a pretty big liability gap there. So that's -- that's it.

THOMAS RICKERT: Thanks very much, Kevin. Let's now move to you, Laureen. Laureen, I guess you're representing a group which has an interest that WHOIS data can be accessible. So maybe you can speak a little bit about the customer side of WHOIS.

LAUREEN KAPIN: Absolutely. And I appreciate the opportunity to be here. My name is Laureen Kapin, and I'm here as a member of the GAC's public safety working group. You gave me a promotion, which I appreciate, but I'm a member, not the chair. And I'm an attorney with the United States Federal Trade Commission. The FTC is the lead enforcement agency on both consumer protection and privacy in the United States. I'm here, however, in my individual capacity. And my views don't necessarily reflect those of the Commission.

That said, what I want to focus on is why WHOIS is important to the public interest, is important for law enforcement and consumer protection as they go about their work to protect the public.

And I also want to speak to the individual public's interest in WHOIS as well. So those two buckets, the law enforcement, consumer protection community and the public community in the importance of WHOIS.

So I'm going to start with the consumer protection and law enforcement perspective. Why is WHOIS important? Why are we here? You've been comparing the issue of WHOIS to longstanding political conflicts because it's something that really is important to law enforcement as they investigate people who are trying to harm the public, trying to harm the

public by stealing their money, by stealing their identity, by invading their privacy.

And what I can tell you is as an attorney for a civil law enforcement agency and also someone who works arm in arm with my criminal law enforcement colleagues from around the world, WHOIS and the information in there is step one -- step one in terms of investigative efforts.

That is the way that an investigator or a police officer can find out who is responsible for a particular website that is involved in unlawful conduct. So, for example, when the Federal Trade Commission is investigating a spyware case, a case where you are on your computer and you may be clicking on a link in an email and that link permits malware to be loaded on your computer which then tracks your key strokes when you're putting in your credit card number or revealing a sensitive health information because you think you're dealing with a pharmacy, we are then called on to figure out, well, who is behind that website.

We will look at the WHOIS for the identity of the registrant. We will look to the WHOIS for the registrar to contact for further information. We will look to the WHOIS even for information we know is inaccurate because fraudsters often use similar

inaccurate information for their schemes which don't relate to just one website but many.

So I use this as a real-world example because it's important for you to know how this information is used.

The other thing I want to emphasize here is that law enforcement agencies use this information because it's available at the moment. I have an investigation -- crucial harms are trying to be stopped by my agency or criminal agencies which deal with issues that can have severe harms, physical harms to the public. And they can access that information quickly. They can access that information for as many websites as they need information about. So it's quick access and it's access in the volume that's necessary to perform crucial work.

Now, if that access is taken away or maybe more -- or made to be accessed in a way that is slow, we are not going to be able to perform our important public work. And I think I heard the word, perhaps, "hampered," but I would say hobbled, I would say cut off at the knees if whatever solution implemented doesn't take the real-world realities that this information needs to be accessed quickly and in an effective manner.

So I wanted to make sure that we're putting a real-world context on this.

Now, I also, as an attorney with a consumer protection agency don't just want to speak on behalf of law enforcement and consumer protection. I want to emphasize you all who use the Internet, which I assume is every single person out there, you have an interest in the WHOIS also. And when I say "public," I don't just mean individual Joe and Jane consumers. I mean businesses trying to prevent their names from being ripped off; banks; charities; pharmacies who have an interest in making sure that their customers aren't deceived or buying counterfeit products. Every single person here has an interest in knowing who they are dealing with when they are forking over their credit card number or sensitive information or sensitive communications.

And when we don't have the luxury of visiting a brick-and-mortar store that's been in our neighborhood for 15 years but instead we are using the Internet for our communications and transactions, then if information isn't posted on the website about who owns it and who operates it and who you can contact if you have a problem -- that's the ideal scenario. But if that doesn't happen, we have this system called the WHOIS that allows you to know who you're dealing with or at least have a channel to figure out who you're dealing with.

And we know at the FTC that the public uses this information. We collect complaints from consumers when they've been ripped off, when they've been subject to harm. And over the last five years, we have found that over 4,000 individuals reporting complaints to the FTC for fraud refer in their complaints to WHOIS information because they use that information to try and resolve the complaint or investigate it for themselves.

So this is really important for the public as well. And if the WHOIS goes dark, which is another phrase I heard on this panel, that has terribly severe consequences for the public At-Large and law enforcement.

And the last word I want to say for now is that the implications of not providing a publicly accessible WHOIS also have legal implications for law enforcement. If this information isn't in the public domain, even if there are solutions that are proposed for layered access or tiered access, there still are consequences, legal consequences, that likely will differ country by country as to the ways in which law enforcement may have to access that information legally, separate and apart from the systems that are proposed. And this has yet to be fully explored.

So these issues are important, and I wanted to be up here to emphasize why it's important in a real-world basis.

THOMAS RICKERT: Thank you so much, Laureen.

[Applause]

And I think this helps a great deal to understand why there is such a need expressed to get access to WHOIS data. We will talk about ways or hurdles to keeping that up based on the legal environment that we're currently facing.

But next to Laureen, we have Susan. Susan, not only are you active on the RDS working group but you are also with the BC. And I guess the BC members are also to a certain extent consumers of WHOIS. So you might want to speak to that as well.

SUSAN KAWAGUCHI: Thank you. Susan Kawaguchi.

And thank you. That was quite an impassioned statement. And most of what Laureen has covered is true for businesses. And we look to our LE, law enforcement, and the FTC for help. Not everything can be solved by an internal security team.

But just a little bit of background. I was on the EWG. I'm a vice chair on the RDS. But I also spent 20 years in the corporate

sector managing domain names and managing the online brand enforcement which also relates for the most part to a domain name and using that WHOIS record. The WHOIS record is a key to any of that enforcement, just simply to reach out and say, hey, did you really understand when you registered that infringing domain name, which is now causing confusion? Or, hey, stop that, this is fraud and this is criminal activity and you knew what you were doing when you registered that domain name with that major brand in the domain.

So it allows you to contact the registrant or at least get some key to their identity. We all knew -- know the WHOIS records are not accurate.

And there's many -- there's large portions of companies that spend lots of time needing to look up that record immediately to fend off attacks on that company and also then work with the law enforcement. So oftentimes, you know, either an eBay or a Facebook security team -- that's my background and experience -- would then provide information, say, look, we've discovered this whole scheme. These are the players but we need your help, too.

So it's a partnership. So if corporations and businesses do not have the ability to protect their brand and protect their users,

then, you know, that need is just as strong as LE because we're partners.

But also WHOIS is not just used for fighting crime. There's a big market out there for domain names. And there are -- and I've spent a long part of my career negotiating domain acquisitions. And there is no way that we're going to deal with someone that cannot identify themselves. You're not going to turn over and offer a substantial sum of money for a domain name if I can't identify that registrant. They have a duty to be -- even if they're using the domain or not, to say, Yeah, this is who I am and I do want to sell this. There's a whole marketplace out there.

There's also M&A. That's not a criminal investigation. That's not a brand enforcement. But you can't buy a company and not be assured that the domain names that are critical to the function of that company are actually owned by the company. And in my experience, it is amazing how many times they weren't. And, you know -- so you had to deal with that problem before you entered into that transaction.

So the WHOIS is used in a lot of different ways. The pressure points that would happen, if you -- if the WHOIS goes away would be extremely critical to doing business and the safety to the users of those businesses.

The other thing is, you know, we're -- the business community is extremely concerned that we will see a patchwork of solutions here, that ICANN won't step up to the plate and lead in this -- though I think they're trying hard -- to develop a model that's temporarily compliant, that can get us through the period that we need to actually put in a system that adheres to the GDPR and all the laws around the world.

And if you look at this diagram here, you'll see here we are November 2017 and the ICANN community with registries and registrars. Then we have the hard deadline of May 2018 that we think something's going to happen. And I understand the registrars and registries. I would not want to be in their position of uncertainty.

So we need in that interim period -- and in the diagram, it goes out to May 2019. I'm not sure how reasonable May 2019, since I have been working on this issue for quite a few years, will we hit that. But it's a date to target.

But we need in that interim period a reasonable solution that works for the registries and registrars, gives the necessary access to the WHOIS records so that we can protect Internet users and is provided -- you know, the contractual issues with ICANN and compliance issues are taken into account but that everybody is doing the same thing. We've already seen the

Dutch DPA say, oh, you can't do this. So we have one model. We don't need a patchwork. We need one solution that we can all agree on as a community and then to move forward. And then probably that solution, the interim solution is not -- people are not going to happy. Somebody's going to feel like in the community this just plain sucks. So we need to move on and -- and we got the PDP fully staffed, working hard, and develop that new solution that's for long-term and that we can have -- make sure we have contractual obligations and the compliance associated with it.

THOMAS RICKERT: Thanks very much, Susan.

Now, Stephanie, you've heard about the needs of WHOIS customers. Now, you're representing the data subjects whose data is publicized in WHOIS. And I should maybe clarify for everyone that GDPR's about the data of natural persons. But that even when you have the field of "company name," that can become personal data if reference can be made to a natural person. So it can basically affect an awful lot of data that's currently being publicized.

So my question to you is: How do data subjects think about WHOIS and GDPR? And let's just assume this community does

not come up to come up with a solution by May '18, how are you going to react?

STEPHANIE PERRIN: Stephanie Perrin for the record.

Thank you very much. I am here representing the Noncommercial Stakeholders Group. And the Noncommercial Stakeholders Group has from the outset of this discussion -- and I would date that back to about 2000 -- been arguing for the respect for data protection law within ICANN. But we also -- as Thomas pointed out, we represent the end users. That includes noncommercial users. Noncommercial users would include very small business but are not corporations. It would include religious organizations. It would include free speech organizations, journalists, women's health networks. All kinds of groups whose rights and human rights are very much jeopardized by an open WHOIS where they are being persecuted for whatever they're doing but who may not have protection under data protection law. Their employees might. These are complex issues that have to be sorted out at a regional level.

So we take the view that we protect them both. Now, this discussion is about GDPR. But I would just like to interject by way of background that I have -- I feel my colleague's pain. I

became a data protection officer for the Department of Communications in Canada in 1984. So my skin is extremely thick. I've been working on data protection issues ever since. It's not popular.

But I was stunned when I came to ICANN in 2013 as a member of the Experts Working Group at the low level of the debate here. And I was familiar with it because when I worked in the Privacy Commissioner's Office in Canada in 2005, I participated in a WHOIS workshop. I believe it was Vancouver. And we prepared a statement, and the commissioner sent a letter. And, sadly, we didn't seem to have progressed very far from 2005 to 2013. And in 2017, we are now doing a massive catchup. And I regard this as a really critical failure to address a risk because not much has changed.

The GDPR is one more step in a logical process of harmonizing data protection law and ensuring that there is good compliance. This was the next step that there would be harmonized compliance in Europe and that there might be fines.

So this was foreseen by just about everybody. So I think this is an accountability issue for ICANN that they need to address.

Now, that's probably enough on that subject. In terms of framing the debate, as I said, it's binary. It's disrespectful. And it

is not making concrete progress on issues that we all care about. I'm on the current RDS group, and I find it -- as I said yesterday, I think Chuck Gomes who's chairing it deserves another ethos award because it requires patience to try to make progress.

This is nonsense. We need to find solutions. We certainly in the Noncommercial Users Group are not trying to facilitate crime. We are trying to facilitate accountable access to personal information and to commercial confidential information in a way that will not jeopardize end users.

And the fact that we are still operating, firstly, most of the debate is about continuing third-party access to data as a purpose for the WHOIS. That is backwards.

The purpose of WHOIS and the purpose of gathering registration data and enforcing that in contracts ought to be linked to ICANN's mission. And ICANN's mission, while we understand the slogan is "One World, One Internet," that does not mean that the entire world should see who has a domain name and that they should have access to their personal information, their phone number, and their address. This is disproportionate.

So how do we move to tiered access in a way that respects end user rights and facilitates speedy access? We know that domain abuse happens within a very critical first few hours of the

registration of names. If we could stop fighting about whether GDPR is a good law or whether data protection will stop the Internet and get down to figuring out how to do rapid access for accredited parties, we would be making some progress. And frankly, I have moved on to thinking about that because nobody's listening anyway. So I'm just going to go ahead and come up with some solutions. And if I may -- do I have another minute to talk about solutions? I really think that we should think about accrediting the users who get access to this third-party data. And figuring out in some other way that is a little more nuanced than having personal versus commercial. As I say, we represent end users. In the kind of economy that we are seeing in an Internet-based world, there will be many, many people working from their homes. We will be fighting for those people's rights. They are not corporations such as Facebook. They are not on the same plane. They're entitled to protection. If they have an idea and they come up with a domain name that they are going to use for their idea, they're entitled to commercial protection without hiring a big lawyer to hide behind. So let's be clear, we have to have a nuanced scale here.

In terms of fighting the abuse, absent a regulatory framework that would figure out who has access, then I think we have to go to standards. The only standards I can think of are quality

standards that would apply in this situation. They would mesh with quality standards for data protection and for security. The other security standards in the ISO stream. If someone has a better idea, please talk to me because that's what we're working on. But please, ICANN has an accountability crisis here. The fact that they have ignored the data commissioners for 17 years and are now only paying attention because there's a 4% fine -- I'm summarizing to be brief here -- that doesn't auger well, from an accountability perspective. Respect for law is fundamental. This is not new. There are 120 data protection laws around the world. They all follow the European model, more or less. And they will be following the GDPR model shortly. So it's time to get down to work. Thank you.

[Applause]

THOMAS RICKERT: Thanks very much. Thanks very much, Stephanie. Now I will turn to Ralf now, and just based on what Stephanie said, that tiered access I guess is an important word to mention, but the question is tiered access to what? You can only offer access to data that you could collect legitimately in the first place. So when it comes to WHOIS, we're talking about owner C data, we're talking about admin C data, tech C data, billing C data, including email addresses, phone number, fax number, and

what have you. So I think we -- as a first step, we need to take a look at what data can legitimately be collected, and you've heard the predicaments that the WHOIS customers are in who would like to establish registration patterns to fight crime or protect users or facilitate domain acquisitions and the like. So Ralf, you're an expert in the legal framework in the European Union. Maybe you can elaborate a little bit on whether there are ways to keep WHOIS as it is, because we've been hearing that over and over again, that there are people in this community who say that we're just need to do -- need to apply the policies correctly and we can things -- leave things as they are. Is this a myth? Is this reality? So maybe you can elaborate -- as a first step, elaborate on whether you think we can continue as we do today. Ralf, over to you, and by the way, I should say, it is extremely challenging to participate in such debates remotely so we really appreciate you taking the trouble of being with us today.

RALF SAUER: Yeah. Thank you very much. I hope everybody can hear me. If chair cannot then -- that's confirmed. Yes.

THOMAS RICKERT: We can hear you all right.

RALF SAUER: Okay, perfect. So first of all, thanks for the invitation. I'm very happy to be able to participate, even if it's remotely. I couldn't -- I couldn't come to Abu Dhabi but I -- I hope this works well enough.

And just to say from the beginning, I'm not an expert on ICANN. I'm an expert on data protection. And I will also be a bit careful as to suggesting solutions at this point, concrete solutions, because I think there still has to be some work on mapping the actual situation and having a clear picture as to the purposes that are pursued with WHOIS and then we're happy to have the discussion and have the discussion also together with the Data Protection Authorities, which I think is an important step that has to be done following the mapping and the clinical analysis.

But I wanted to say -- I mean, make at least a couple of points I think that are important in the debate. First of all, and that follows up on what the colleague from the FTC has said, we're fully aware of the public interests involved in that. We recognize that there are important public interests. I think there is no question about that. And it's important to realize from the outset that the GDPR, as well as the current data protection rules, also do that. They also recognize public interests and this kind of balancing is in a way baked into our rules. So that's also

not something which should be forgotten. It's not a one-sided law, if you wish. It's a law which went through a difficult process of discussions. It was probably the longest debated law that we ever had, and all sides were represented in the debate and therefore also all interests were taken into account when designing that law. And as -- and I'm happy here that I can follow up on things that were said by Nick and Stephanie. First of all, it's -- I think we should -- while we see the public interest, it's also clear that not everybody who registers is a fraudster or a criminal. So we're talking here about privacy interest of individuals, a legitimate privacy interest. In the EU this has a Constitutional basis. It's a fundamental right. But not just in the EU. These principles are recognized at international level and in many, many countries around the world. And I think Stephanie said it well. The model that the EU is pursuing is also pursued by many countries around the world and increasingly so. And it's also more and more reflected in international standards such as, for example, the Council of Europe Convention 108. It's in EU recognized for -- am I -- yeah. It's in EU recognized for more than 20 years, and that's why those are not new questions. Not at all. This is not a GDPR question. The only thing that might change that indeed is there is now a possibility to have sanctions. But the compliance issue, if there is a compliance issue and to the extent there might be one is around for many, many years. And

our Data Protection Authorities have been engaged with ICANN for many, many years. I've seen letters and opinions from the Data Protection Authorities which have been very willing to engage on this topic and have repeatedly said so since 2003. So that's by now 14 years ago, and they have done so almost every two to three years. They have written and made statements and offered their help in this. So I think that's -- that's also something that needs to be on everybody's mind.

So this is not a GDPR issue. The GDPR is not yet affected, but the important thing is that it represents a lot of continuity. And on the principles, the core principles that are discussed in this context, they are all old. And nothing has changed on these principles of purpose limitation, legal basis, accuracy, data retention, data security. This is all already in the current law, and it is there for -- in the European Union, at least since 1995. And in fact, I would even say that the GDPR improves the situation in the sense that it creates a harmonized, fully harmonized legal framework. As Nick explained, we currently have a directive in EU law that means it -- it's a law which gives the overall broad framework but this has to be implemented, transposed by member states, and they have certain flexibility in that. That's different now. It will be different now as of next year, because we have a regulation. The regulation is itself the

law, which needs no further transposition or implementation. So it increases the harmonization, and there are mechanisms in the GDPR also for ensuring a harmonized interpretation and therefore application of the GDPR. Something which is called a consistency mechanism whereby Data Protection Authorities will in the future, in a much closer framework, coordinate their actions and their interpretation of the law. So that's actually a positive step. It's -- it will make -- make it much easier for -- for operators like -- such as registrars and registries to know exactly what is the law and how is it applied be by the forces which are the Data Protection Authorities. And the GDPR also creates new tools that might be helpful, for example, codes of conduct which is something which one can perhaps also think about as a bottom-up way to find rules that are specifically designed for an industry or a type of business operation. And this, of course, has to be done in cooperation with the Data Protection Authorities and might also be worth thinking about.

I also wanted to say something about the international dimension because the chair had referred to that. But I -- I'm afraid to say not in a fully accurate way. The GDPR does not apply -- will not apply in the future to everybody who can be reached by customers from the EU or who offers services to the EU, no. The rules will only apply if operators that are not

established in the EU specifically target EU customers. And we can talk about what that means. So also in that respect, I think we should be a bit more cautious when it comes to interpreting or making statements out -- about our new rules.

Last point on this maybe, sanctions also there, I think let's -- let's be a bit more rational and calm here. We always see these references to maximum fines. It's not sure at all whether there would be any fines, whether the Data Protection Authorities would take that route and they would have to take into account many factors and that includes in particular compliance efforts and other things. But in any event, compliance as such is something I think which is normal. I -- and this does not just apply to data protection rules. This applies to any regulatory framework, of which there are many. Data protection should not be seen as something special or different from other fields.

Just a -- maybe a few words about the elements that we are talking about here. This is not something which is -- which is, I think, too complicated or too difficult to understand. And first of all, we are only talking about personal data. So to the extent that WHOIS also concerns other type of data, maybe that of -- that relates to legal persons or companies, that is not something which is an issue. And then the principles that apply I think are also easy to understand. This is about what we call purpose

limitations. So since we are talking about an interference with a fundamental right, it has to be clear for which purposes this is done and the purpose is then also important for, for example, knowing what is the legal basis for that. Again, the legal basis that one has to have something like this is quite normal when you are in an area where we're talking about an interference with a fundamental right. I think we know this. Everybody has done constitutional law, I think that's something that you need to have. And that is, again, common to many systems around the world. And then other principles such as data minimization, that you should limit the data to what is necessary. Accuracy that that data -- data retention, so the data should not be kept for longer than is necessary. All of this follows from the general idea that personal data should be protected to the extent necessary and possible.

And I also wanted here to make at least one remark. I mean, I heard a lot, especially from the colleague from the FTC about accuracy of the data and the need, therefore, to check. I have the impression maybe there's also a need from the start to improve a bit the systems for ensuring accuracy. If that is a major issue, then I think one should also work on that. And then maybe there is less of a need to check afterwards. I think the

initial verification and maybe the ongoing verification is something which is quite important here.

THOMAS RICKERT: If you could wrap up very short -- briefly.

RALF SAUER: Yes. Our recommendation, or what we think is the way forward, and I have seen this now already reflected also in a number of papers that have come out in the last couple of weeks, I think it's important to map the situation, to know exactly what -- for which purposes WHOIS should be used and needs to be used. That is the basis for a comprehensive analysis, and we see that law firms have been -- been, you know, involved in this, specialists that look at this, and we're happy to be involved in that discussion. And then I think on that basis, when this is mature, then there should be a dialogue with the Data Protection Authorities and again, we as a commission are more than happy to facilitate that dialogue and be involved in that. We are a member of the group of Data Protection Authorities, not a voting member but a member nevertheless. So we are there -- we are ready to work constructively on this with caution a bit against some of the alarmist statements that are made. The data protection -- our rules provide a number of tools to

address the issue and solutions can be found. As I said, the balancing with public interest is baked into our rules and, therefore, our rules allow to accommodate these interests. Thank you very much.

THOMAS RICKERT: Thanks very much, Ralf. Quick follow-up question. Yes or no answer, please. Just one word, yes or no. Is WHOIS in its current form sustainable?

RALF SAUER: I think --

THOMAS RICKERT: Okay. I guess that answers it. Thanks very much. No, we -- I think we have --

RALF SAUER: This is exactly the kind of question which leads to alarmist statements, I think, later on. The question is exactly for which purposes and on which basis and this needs to be analyzed. I'm not going to tell you now. This is not possible.

THOMAS RICKERT: I --

RALF SAUER: I think legitimate users will continue to be possible, yes.

THOMAS RICKERT: Thanks very much. I couldn't resist the temptation of asking a binary question to a lawyer, which is always a -- always a challenge. I'm a lawyer myself, so we can be happy to at least have two different -- two opinions when you have two people in the room. Sometimes it's more. Thanks so much, Ralf.

Now let's move to Goran.

Goran, I know that ICANN has done some outreach and engagement in Europe. I guess the community is very interested in hearing what the outcome of those discussions was. I think you've also asked for more time to implementing the changes that need to be considered. So is there any feedback that you'd like to give to the audience?

GORAN MARBY: I think I over the last week have shared all the information I have about everything.

So remember the first thing we did was to go out and sort of socialize the fact that GDPR could have an effect on WHOIS. And we talked about that in, I think, Johannesburg. We talked about that in Copenhagen. I talked about it (indiscernible). It was really the starting point for process.

So the interactions -- and one of the things you helped me with was get in user cases. The user cases have two -- had two meanings. One of them was because the way the GDPR is set up, the user cases are important for us -- for anyone to look at the usage of the WHOIS data. So that became something we channeled over to the Hamilton law firm.

The other part of that is we sent a letter to all the DPAs in Europe where -- I have to calculate here. I received, ah, one answer which I got yesterday. We will publish that answer very, very soon.

I mean, to the defense of the DPAs, it's very hard legally for a DPA to make an advice before they make a decision. Apparently we talked about it. There's never been in the European context I know any legal actions from a DPA against a WHOIS as it is today. Could be good for you to know that.

And before I just proceed, just to point out one thing. The discussion that has been around here, I haven't been around

that long but I have a feeling that you've been discussing this before. I get that feeling in the room sort of.

[Laughter]

Could be so.

I'm talking from my perspective is strictly compliance with the law. I don't take sides in the discussions which belongs in the community about the usage or the privacy of WHOIS. And I want to make that very, very clear because I think it's important for the community to continue that discussion in every shape and form. So we will share the answer from that.

The next level we did was then, of course, to send the letters -- to send the information to Hamilton and then we published that information. And we accidentally started to change what we said. Instead of saying we might think it's a problem, we now say -- the next version of that, we said depending on the information we now have, the GNSO also did something. We then went out and said we think it's going to have an effect on WHOIS.

And why am I so technocratically boring? The reason for that is I'm concerned about the partners involved. So if we say you are doing anything, we can create additional problems, for instance,

for the contracted parties and for ourself, which is I have to be careful in how I say things.

And then we also did other engagement activities. Because ICANN is a large tent, we reached out to law enforcement, the European Commission, but also the privacy side to talk to them and make them aware about the situation as I'm bounded by the policies set by the community, which I can't change. And, therefore, it's important that everybody has their say.

So, we also added speaking points on top of that, is that we now think that the compliance -- because of what we are now saying, we also think potentially that this will have an effect on our compliance which means that we will not be able to fulfill the policies set by the community based on the knowledge we are having right now.

So the role we're in right now is that we're asking everybody to provide us with legal documentation and questions which we can provide to Hamilton law firm. And after that, we will come back and our intention is in close cooperation with -- if you excuse me saying that, both sides of the story to make up proposals for how we can be compliant to the law.

And we will ask -- and we are thinking of coming out with sort of three models. Why do we talk about three models? Because in

Europe right now there are at least three models how the CCs are actually handling this. And because there's a good relationship with local DPAs, we think maybe that could be a starting point. And I also know -- and I really want to thank the community and everybody involved, it's been a fantastic week with all the engagement that has been had.

After that, I have to make a decision. And it's my decision because I have to make the decision how ICANN, if we are a data controller, could be compliant with the law. We cannot then have two different compliances, one that we think we're compliant with the law and the other one how we ask the contracted parties to be compliant. So at that point, we will say that this will be how we will use our compliance going forward.

I urge the community as well to continue the discussion about WHOIS in a broader scale in the policy work as well. So that's the format for it. And I received a question. I received one question. Remember also that the board already -- was it last week? Yeah, it was. Last week took a decision that we are going to postpone the implementation of thick WHOIS. And one of the reasons for that is the uncertainty with GDPR. And the decision was to postpone it for three -- no, sorry, six months, 180 days. So we're already taking actions.

And if I have more time later, I also have a statement to do -- to read about how we're going to deal with our compliance in the meantime. But in respect too all the other speakers, I would like to leave the microphone now.

THOMAS RICKERT: Thanks very much, Goran.

The next question is for you, Becky. We had a couple of legal analyses that spoke to the potential role of ICANN as data controller. And I think what's important for the audience to understand is that as of May 2018, the contracted parties, and specifically the registrars, will need to have additional information duties. So they need to explain the roles and responsibilities of those involved to the data subjects.

And so far ICANN has not confirmed that it has the role of data controller, but I guess we need to start somewhere to establish the roles throughout the whole value chain.

So are there any plans on the side of ICANN to make proposals? I heard Goran said that there are three models underway. But is that something where the board plans to engage with the contracted parties? Or can we expect something from ICANN developed in isolation?

BECKY BURR: So, first of all, I want to associate myself with the comments of the registry and registrar representative as a member of the contracted party, and particularly the comment about "I must have done something terrible in my life to have spent the last 20 years on privacy and ICANN and ended up on the board in this moment."

This is -- this is, as Goran said, a compliance issue. It is, therefore, in the org's sphere of competence and not something that the board should interfere in.

However, there is a board issue here. And I think -- I can clarify -- I'll tell you what I think. We've been told by three different law firms and the Dutch data protection authority that free public access to all WHOIS data is not compliant with European law, period. That's what they say. The Dutch data protection authority gets to stand on that position and impose it on registries and registrars.

Contracted parties must -- and they will -- comply with applicable law. And ICANN can't compel them to comply with the contract in violation of applicable law.

From the board perspective, we have to think about what are the implications for ICANN and the multistakeholder model if we

do not find a legally compliant solution that facilitates appropriate access for legitimate and proportionate purposes. And we ought to stop talking about all of the other stuff and get on to that. So I think that's my message. I'm an individual board member. And I think -- and as Goran said, I think we've made great progress here. Let's capitalize on it. I think Stephanie's point about the need for a reasonable credentialing process is critical.

ICANN will be coming up with a model. That from a board perspective is critical to moving the discussion forward and ensuring that ICANN and the multistakeholder model survives the GDPR.

THOMAS RICKERT: Thanks very much, Becky.

Goran, you have a quick followup because then I would like to move to Q&A.

GORAN MARBY: I have a statement to read and I have to read it. And I think it's a sort of interest for at least the contracted parties. I can wait and talk about that some other day, if you want to.

THOMAS RICKERT: Now, you are putting me as a moderator between a rock and a hard place. But if it doesn't take too long, by all means, please, please go ahead. But then I would really like to take some questions.

And for the organizers, I'd like to know whether we can have a few extra minutes because I think you do want to ask some questions and make some comments.

GORAN MARBY: So we received a question how we're going to handle compliance during this period until the lawfully comes in place. And this is something that we've been thinking and talking about.

So -- but just to give you -- I have to do this, I have to say some things in this one. First of all, I have no right to change any policy. I have to work in the measurements set by the community. And that's important in anything we do.

And the policy -- the current policy says there are things in the contracts that makes -- that there are things that the contracted parties have to put in place for WHOIS. So that's -- that's sort of the benchmark I'm using. We cannot accept to go away from a full WHOIS.

But during this period of uncertainty and under the condition noted blow, ICANN contracted compliance will defer taking action against any registry or registrar for a noncompliance of contractual obligation related to the handling of registration data. But to be eligible for this, a contracted party that intends to deviate from existing obligations must share its model with ICANN.

Contract compliance and the Global Domains Division. To the extent that the party requests confidential treatment, ICANN can remove any identifying information and share only the elements of the model with the Hamilton law firm for the purpose of legal analysis against requirements of the GDPR.

The model should reflect the reasonable accommodation of existing contract obligations and the GDPR and should be accompanied by analysis explaining how the model reconciles those two.

For clarity, contracted compliance would not abstain from enforcement if, for instance, a contracted party submitted a model under which it abandoned its WHOIS obligations. In addition, a model that satisfies the condition noted here may also require compliance with other contracted obligations or consensus policy. Example, giving the registry services evaluation policy.

A model may also require further modification if it's later determined not to comply either with the GDPR or any future community-developed policy. Thank you.

THOMAS RICKERT: Thanks very much.

GORAN MARBY: This letter will be posted tomorrow.

THOMAS RICKERT: Thanks very much, Goran.

[Applause]

I guess it's great that you clarified certain elements of the next steps. I would have tons of questions with respect to the statement, but let's move to the audience.

I know that there are questions in the remote participation room. And I would like to ask you to take the microphone in the middle of the corridor.

A couple of ground rules for Q&A. Please state your name and your affiliation. Please also make clear to whom you're directing

your question, if it is a question. And we're going to use the two-minute timer and I will be quite strict on enforcing it. Thank you.

So the first question comes from a remote participant.

REMOTE INTERVENTION: This question comes from Maxim Alzoba of FAITID. Does GDPR protect residents of the E.U., too, as a non-E.U. citizen?

THOMAS RICKERT: Nick, do you want to take that one?

NICK WENBAN-SMITH: I think it's an easy one. Yes.

THOMAS RICKERT: He's a lawyer. Yes, no. Great. Steve.

STEVE DelBIANCO: Thank you. Steve DelBianco with the business constituency. The way you've described this is being in this room on this issue at this time is Dante's Inferno. Help us understand the path out of it.

So question for Goran and Becky, representatives of org. You're the middle row on the diagram. Those of us in the room are the

top row, the broader community. So in the middle row at ICANN org, do I have it right you are going to work with lawyers as well as contract parties in the community to come up with an interim compliance policy that could be potentially based on models like Amsterdam's using today, or .EU. While that interim compliance policy is being enforced, the interim period compliance, at the same time the rest of us in this room are supposed to get busy on the top row at pushing ahead with the community-based policy development to arrive at the point where we have a new registrant data service, or RDS. At that point, the community comes to the org and says, Help us to implement that. And that replaces the interim compliance based on a model that you will have enforced over the interim period. So if I've got that wrong, please correct the record because we need a path out of hell. And so far, we're not seeing it.

THOMAS RICKERT: Thanks, Steve.

Goran?

GORAN MARBY: You are right and wrong and maybe. First of all, you're wrong. We're not going to do -- we're not going to do another policy.

This is about compliance. That's a very big difference. It's a very big difference between us coming up with something that is even related to policy. And the reason why -- we actually are having an argument. You can't hear it because he doesn't have a microphone. Thank God.

It is so important for me -- and I say that again. The guidelines -- it's not -- the guidelines that are set by this community are the ones that we follow. That's the one we have to follow. So we have to -- we are working on the compliance issue.

That will create a misfit between the policies that is set by the community and our ability to enforce it.

So I think it's a good idea for the community to come together and think about that. But that's your decision, not mine.

And as you well know, we have -- the only reason why I haven't set a time line here for what we're doing is because you actually asked me to grant you a little bit more time to come in with legal questions that we can transfer into Hamilton.

I know I sound harsh. I know I sound scary on this one. But as I usually say with a bass voice, we are talking about the law.

THOMAS RICKERT: Thanks, Goran.

Chuck is next and let's try to keep the answers to maybe a maximum of one minute so that we can hear more comments from the floor.

CHUCK GOMES: Thanks. Chuck Gomes speaking mostly with regard to registry contracts and also maybe a little bit with regard to being chair of the RDS PDP working group. Looking at that middle item called interim compliance policy, I'll just check maybe something that Goran said there. And he's accurate, I think, that he doesn't have the authority to do it but the board does actually have a right to establish an emergency policy. But he's absolutely right that it's really not a consensus policy as that is defined. But there still is a right to do something there. And whether that's used here or not is another issue.

With regard to the -- I mean, the RDS PDP working group is tasked with coming up with a consensus policy and making recommendations in that regard. And personally, as chair of this working group, all the stuff I think is very helpful to what we're doing, even though it's a separate track.

Goran is doing a good job of communicating with us. I think we're all in this together. And we appreciate everything that's happening.

[Applause]

THOMAS RICKERT: Thanks very much, chuck. I guess that was more a statement than a question. Let's now move to the next one in queue, please.

ANDREAS DLAMINI: Thank you. Andreas from the GAC, speaking on my own behalf. It's good to hear different sides of the debate even though we're not coming to an answer as yet. In 2013, I dealt with a case whereby someone in some continent registered domains across all the available TLDs -- gTLDs at the time on my king's name, first name. And they registered them across all the gTLDs. And then they went on to register the king's mother's name across all the available gTLDs and on to register his father's name across. And then two years after registering them, they started to sell these domain names to us.

Now, I was given this case to deal with. When I started to look into it, my first point of call was to go to the WHOIS to try to make up a case to take it up with -- through the UDRP. I don't know if it is still called by that name.

And, okay. You have to have this information when you make that case through the UDRP. You have to have the name of the registrant. You have to have the address of the registrant. You've got to have all these contact details for this registrant.

Then the question is, had this information not been available in WHOIS, what was going to be our avenue to try to address the issue. Thank you very much. And I expect ICANN to respect the accreditation -- the RAA with its registrars. Thank you.

THOMAS RICKERT: Thanks very much for that. And I guess it's good of you to note that there's an impact on rights protections mechanisms that need to be considered as well. I suggest we go to one remote question and then back to the queue. And just to let you know, we have been granted an additional 15 minutes. But should you add yourself to the queue in the room, you might be disappointed because we can't get to you. The remote question, please, James.

REMOTE INTERVENTION: This question comes from Kristine Lanki. Was there a specific problem concerning GDPR and .JOBS?

THOMAS RICKERT: I think we're going to note that question to be answered in writing later. Thanks very much. Pierre.

PIERRE BONIS: Thank you. Pierre Bonis from AFNIC, .FR and several gTLDs as a backend. I just wanted to make two quick comments. First of all, thank you, Goran, and thanks to the board to have opened the possibility for registries to ask for waiver to be able to be compliance with the law. I think this is a very, very good move, and we were expecting it for a long time. And the second comment I would like to give, it's more a sharing of experience. And under .FR, we have a little bit more than three million domain names, and we have 400 requests per year to access the full data and this request not coming from IP law firms and law enforcement agencies. 400 out of 3 million domain name. And they are treated in less than one day. So it seems that it's feasible, and this is not maybe the nightmare that someone fears. That was just the cool experience I wanted to share with you.

THOMAS RICKERT: Thanks very much, Pierre. Alan.

ALAN GREENBERG: Thank you. It's not a question; it's a statement. I guess I'd like to express a great amount of frustration, and I agree with much of what Susan, Laureen, Stephanie, and Chuck from the -- this microphone said. There's a lot of steps, there's a lot of parts to this process and fixing it. We seem to be serializing it and saying we have to do one part first, then we'll think about the next one, then the next one. We have -- in the programming world, we have better techniques than the ones we used in the 1970s where we did one step at a time slowly and progressed one to the other. We need to do -- have a lot more parallelism. And there's lots of parts of this -- this process we can do now, even if we don't know exactly how it fits into the other parts. And be ready a lot quicker than we will otherwise. Thank you.

THOMAS RICKERT: Thanks, Alan. Please.

NIGEL CASSIMIRE: Good day, everyone. And thanks for the good information that's coming out of this forum. My name is Nigel Cassimire from the Caribbean Telecommunications Union. I'm gathering that there's something called a legitimate user, but I'm not clear on what that might be. And I'm wondering what -- what categories of user, of existing user that that might possibly exclude in

future. So if I'm an individual who's just checking to see whether a company that's online is who they say they are or I'm a student trying to do some research on the domain name industry or something of this sort, am I likely to be a legitimate user that could get access to this information, and if not, what recourse might be there for me? Is this that I need to go to get services from a legitimate user to find out the information or what? I'm a little unclear and wonder if I can get some clarification on what this legitimate user might be.

THOMAS RICKERT: Thanks for the question, Nigel. I guess the answer at the moment is that we don't know. We have to define, first, what data can be collected, collect it, and then revealing the data to third parties is yet to be determined, whether there is a specific legal basis or law required or whether it can be done otherwise. I'm not aware of any truly assessed model that would allow for tiered access but tiered access is certainly something that needs to be discussed. Thanks so much. I know that we have two more questions from the remote participants. James, let's take the next one and then move to Milton.

REMOTE INTERVENTION: This question comes from Bonnie. Is ICANN going to be reacting to all laws passed by other jurisdictions? Why is Europe specifically getting attention? We have laws passed in other countries but they are not discussed. Is ICANN bound by European law or not? Also, what the EU proposes is also going against other jurisdictions' data laws. Which one takes precedence?

THOMAS RICKERT: Thanks very much. Becky has signaled that she's willing to take that question.

BECKY BURR: The way that GDPR works is that any processer established in the European Union must comply with GDPR and any processer established outside of the European Union, so a registry or registrar or ICANN, must comply with the law with respect to EU residents, this doesn't have anything to do with citizenship, insofar as they are reaching in and offering services in the EU. That's really not -- people sometimes complain about this being extra territorial. I would just point out that that's actually not the way very many -- that's not different from the way very many laws work. If somebody was advertising to U.S. consumers products that violated the -- you know, that were deceptive or

created problems for consumers, if they were doing that in Canada, I would expect the Data Protection Authority in Canada to -- or not the -- the consumer protection authority in Canada to say it had the right to protect its -- its residents and people who -- against people who use practices that are against the law in the country. But -- so it applies basically to anybody -- for all data to anybody who's established in the EU and all data about -- personal data about EU residents for most anybody else.

THOMAS RICKERT: Thanks, Becky. I guess the second half of the question, whether -- why we're just looking at European law and whether there are other laws underway, I know, Kevin, you've done research on that. Is there anything in the queue that would establish higher hurdles than GDPR?

KEVIN KREUSER: Yeah, we've looked at, I think, about 46 countries across different parts of the world and comparing them to GDPR because we get asked the same question just as a company. When implementing, you know, technical solutions that are necessary on a GDPR, are we going to then have to do something different in the rest of the world. And for the most part -- and there are nuances to various laws, and this includes even

updates to new laws, proposed laws -- the GDPR is a pretty good bar to work off because it does set a high standard. There's also 64, I think, countries in the world that have adopted Convention 108, which has the same basic principles of privacy as the underlying foundation. So you may have nuances in these various laws. Turkey has some weird thing about data transfer. But nothing that I've seen that would -- would cause a problem if we adopt a kind of GDPR global solution that couldn't also be resolved through the -- the conflict mechanism that everyone loves so much.

THOMAS RICKERT: Thanks very much, Kevin. Milton, please.

MILTON MUELLER: Milton Mueller, Georgia Tech, Internet Governance Project and noncommercial users constituency. I have to say as an American I was extremely disappointed with the intervention of the Federal Trade Commission which is supposed to be responsible for privacy regulation in the United States and we heard a ten-minute harangue about the convenience of having access to WHOIS data without a single mention of their privacy mandate. But I think that leads us to the more significant issue I want to address, which is, we have to stop pretending that the

fact that people are now using WHOIS data for certain things means that whatever solution we come up with has to accommodate all of those uses. The origin of data protection principles lies in the purpose. You can only collect data for a legitimate purpose. And I think a lot of the discussion of the reforms of WHOIS that we're getting into are getting this backwards. We're starting with existing use cases. They're not just asking as a starting point, why are we collecting data for ICANN? Why is ICANN -- what is ICANN's purpose in collecting this data? What is it needed for? The fact that it then collects this data and then publishes it and people find that data convenient doesn't mean that that's the purpose of their collection.

So I would also like to remind us that we had this debate in 2006 about what is the purpose of WHOIS. The GNSO Council actually came to a two-thirds majority position on the definition of the purpose of WHOIS, and that two-thirds majority was simply overridden by back room dealing between the GAC and certain people within the GNSO. We might want to go back and look at that discussion and come up with a nice narrow technical definition of the purpose of WHOIS. Thank you.

THOMAS RICKERT: Thanks very much. Pretty much on time, Milton.

[Applause]

Laureen, you'd like to respond to that.

LAUREEN KAPIN: What I want to emphasize is that the FTC, just like the ICANN bylaws and the 2007 GAC principles and the GDPR itself, tell us there is a balance to be achieved between law enforcement interests and the interests of the public and privacy interests. And if you've misinterpreted my remarks to say that there aren't legitimacy -- legitimate privacy interests, you've misunderstood what I had to say.

We at the FTC protect people's privacy in a variety of ways and I wanted to make sure people understood how we use the WHOIS to do that. We also realize that the WHOIS can be misused, and, in fact, ICANN has instituted policies to prevent folks from scraping the WHOIS for illicit purposes. And we absolutely advocate that those policies should be enforced. But what I want to emphasize is that there is going to be a real world practical impact if this information is not available in a balanced way to law enforcement and the public. And I want to make that clear.

THOMAS RICKERT: Thanks very much. Let me just remind you that we have 8 minutes left and we have to stop on time. So Margie, you're next.

MARGIE MILAM: Thank you. Margie Milam with Facebook. I wanted to comment about the statement that Goran read. Thank you for sharing it. I recognize how difficult it is for the ICANN org to sort through these issues, but I think it needs further discussion. I'm struck by the fact that the statement fragments the approach to WHOIS and doesn't provide any leadership or direction to help the registries or registrars that have to do something in this interim period. One of the things as I think about this issue is that ICANN could, for example, help the registries and registrars come up with something that's a little more standard, if you will. And there are tools in the GDPR that allow that. For example, there's the Code of Conduct that hasn't been explored, to my knowledge. I think that that might be a way where you could provide some guidance and the industry could come together so that there's one solution during this interim period instead of having multiple ones under the approach that ICANN org has suggested.

So one of my suggestions for the organization is perhaps you could consider a public comment period on that statement and

see if there's a way to come up with an approach during the interim period that makes it a little more open to community input and perhaps provide more instruction and guidance to the contracted parties. Thank you.

THOMAS RICKERT: Thanks. Thanks very much. Goran, would you like to react to that?

GORAN MARBY: I just want to point out that we have had -- first we asked for the user cases. And now we are asking you for help us with the legal advice. And third, we are asking -- we are going to -- in the compliance process we're asking for comments on the three -- on the three different models we're proposing. So I think that we're completely in line. Thank you very much.

THOMAS RICKERT: Thanks very much.

OWEN DELONG: Owen DeLong, Akamai, speaking primarily for myself. First, I want to commend Goran and the board on the statement that Goran read. I think it will provide a lot of relief to registrars and

others in the community that are affected by this. And it's pretty much what we were asking for in the joint session with the board.

Second, I want to point out that I think the use cases are a perfectly valid approach to this. I think that Milton's desire to declare arbitrary use cases illegitimate through the subtext of what he was saying is somewhat confusing to me from his previous statements, but I -- I think that we do need to look at all the ways in which WHOIS is being used in order to determine what we want to state are the legitimate purposes for WHOIS and why we collect the data going forward

THOMAS RICKERT: Thanks very much for your statement. And maybe you can go to the operator and state your name there so that we can add it to the record because the name was indiscernible. James, let's take another remote question.

REMOTE INTERVENTION: This question comes from Maxim Alzoba from FAITID. Does GDPR recognize the special role law enforcement agencies outside of the EU in their respective jurisdictions on their soil? Usually they're exempt from some sort of data protections locally.

THOMAS RICKERT: Is there anyone on the panel that would like to take the question? I would suggest that in the essence of time we'll get back to that later on. And congratulations, Maxim, for hacking the speakers order by sneaking in twice remotely. Beth.

BETH BACON: Beth Bacon from Public Interest Registry. I want to appreciate everyone's time. It's very clear we are in violent agreement that GDPR is an issue and that we have some questions. Goran, I wanted to ask a specific question with regards to your statement. It's more practical and a little more narrow than just WHOIS. Will that apply to other aspects of our requirements as contracted parties that are impacted by GDPR such as retention and escrow data transfers or is that specific only to WHOIS? Because I think if that's true, we may be seeing a lot of proposals for some very thin WHOIS models. Thanks.

GORAN MARBY: What we're asking for is to share the models you think are a problem. And I want to repeat something I said before. Our contracts can never supersede any local laws. And there is a process within the policy and implementation how to deal with that. And we always dealt with that. So I think we're going to

continue this one. This was about -- the statement is really about the WHOIS. But we also -- we are dealing with some unknowns which we all know here. There are things that we don't know. Really want to have your information going forward. But the statement is related to the WHOIS, which I said in the beginning. And we will be publishing it on ICANN org in a way that you actually can find it, I suppose very soon. Today or tomorrow. Thank you.

THOMAS RICKERT: Thanks very much, Goran. To my knowledge, we have one question from a remote participant left. So James. Fire away.

REMOTE INTERVENTION: This question again comes from Maxim Alzoba --

[Laughter]

THOMAS RICKERT: Okay, I think Maxim had his fair share. By the way for everyone, he's sitting in the first row over here. So I guess then it's time for us to wrap up. I'd like to thank the audience. Goran.

GORAN MARBY: I had one more thing I want to say. One of the things that has been very, very important for me in this and when I engage with DPAs or anyone else, the credibility of the multistakeholder model is very important in those discussions. There are rooms that I would never have been able to enter if I couldn't reference the multistakeholder model the way we work. It is important that we keep that in mind because if we're not, we're just special interests. The multistakeholder model gives us the credibility to have discussions with several partners within this framework and other ones. So thank you very much.

THOMAS RICKERT: Thanks very much, Goran, and I think that's a great segue to my closing remark and that is, we have the multistakeholder model. The community needs to be coming in in the phase where the policy is revised. But in the interim period, that's my take-away from this session. This needs to be dealt with as a priority contractual compliance issue to avoid sanctions from DPAs and allowing for compliance. And I would hope that, at least from what I heard from the contracted parties, that ICANN does not just propose something to the community but there's going to be a true dialogue on how this joint responsibility can be fulfilled.

Now, let me thank, first and foremost, Ralf joining remotely. I know this is extremely difficult. Let me thank the excellent panel, and for those who can see this table, you know, even though you have been disappointed with the outcome of the session, we're doing pretty good on gender balance, don't we?

[Applause]

And with that, I'd like to thank you all for your interest. We're going to surely follow up on this discussion. Have a great day and safe travels once this meeting is over.

[Applause]

[END OF TRANSCRIPTION]