COPENHAGEN – Cross-Community Discussion with Data Protection Commissioners
Monday, March 13, 2017 – 15:15 to 16:45 CET
ICANN58 | Copenhagen, Denmark

NIGEL HICKSON: Hello. Good afternoon, ladies and gentlemen. Could -- oops. Sorry. Good afternoon. We'll start this session in a few minutes, but could people -- could we encourage people to come to the front? We're not contagious, so if you'd like to come to the front, that would be great. Be collegiate.

JAMES BLADEL: Good afternoon. If we could have folks take their seats, we'll get started, as Nigel was saying, please feel comfortable coming up front. We have lots of room here and perhaps the room was a little optimistic for the audience. But please feel comfortable to come up to the front rows. We'll get started here in about a hundred seconds.

So good afternoon and welcome to this cross-community discussion session. Our topic today focuses on data privacy and is jointly hosted by the GNSO and the Government Advisory Committee.

Today, we are honored to be joined by our guests representing data protection experts in the Council of Europe, and on behalf of the entire community, please join me in welcoming these newcomers to ICANN Copenhagen.

[Applause]

JAMES BLADEL: The topic of data privacy affects all stakeholders, whether we represent the interests of governments, domain name registries or registrars, or if we are among the millions of domain name registrants and end users here in Europe or around the world.

In nearly every aspect, protecting data privacy impacts and challenges the work that we do here at ICANN, and this session, in particular, comes at an opportune time as we in the GNSO are currently engaged in policy development work that's examining the future of the registration data system entirely and I'm hopeful that this session will aid and inform that work and that our discussions today will kick off the beginning of a continuous collaboration and an ongoing dialogue with all of your organizations.

So with that said, let's get started on what I expect will be an engaging session.

At this time, I would like to welcome Johannes Kleijssen from Council of Europe. He's the Director of Information Society and Action Against Crime and he has a few opening remarks. Director Kleijssen.

JOHANNES KLEIJSSEN: Thank you very much, Chairman. Thank you. Thank you, James. Good afternoon to you all. Very grateful to the GNSO, GAC, and the ICANN board for having us here and for having supported the Council of Europe's proposal for this cross-community discussion.

Perhaps a few words on why the Council of Europe, who are we. I promise I'll be just one or two minutes.

47 states and 5 observers based in Strasbourg, France, set up in '49 dealing with human rights, rule of law, and democracy. Civil society has been with us now for some over 30 years, and we're currently also setting up a platform for cooperation with the business community, giving them a formal status and seat at the table.

So increasingly, the Council of Europe is turning from a purely intergovernmental organization to a multistakeholder body, not unlike the one we are speaking here to today.

Those of you from Europe will, of course, have heard about it. Those of you who are from outside may have heard about the European Convention on Human Rights and the court in Strasbourg which gives binding decisions on individual human rights cases, but to reassure also those that come from law enforcement, we have over 60 international conventions dealing with criminal law matters, so we very much deal with both.

We've had observer status with the GAC since 2010 and have so far submitted three specific reports for discussion, one of which is being discussed this very week.

For today's session, of particular relevance is our data protection convention, also called Convention 108, which brings together 50 parties, 50 states that have ratified the convention, and soon 10 observers, which means that with the 60 countries that regularly come to discuss data protection matters, we bring together half of the world's states that have data protection legislation, so well also beyond Europe.

The counterpart, perhaps, to this data protection convention is the cybercrime convention, also known as the Budapest Convention, so far the only international legal instrument in this field. It also has 50 contracting states, including, for instance, the USA, and we have been -- we are working with some 125 countries around the world on capacity building.

For today's event, we very much hope that this discussion will be the start of a process, not a one-off event. We are convinced that it is both timely and necessary to have this discussion. I hope those of you that may still be skeptical will be convinced, after today's discussion and after having heard from the data protection commissioners and other experts, that it is a necessary dialogue.

There are increasingly conflicting legal obligations of contracted parties between their obligations vis-a-vis ICANN and national and international law. This also applies to ICANN itself. And we hope today's discussion will be the beginning of a process that will lead to meaningful multistakeholder solutions. Thank you very much.

BECKY BURR: Thank you, and welcome everybody. Many of you know that my professional life has been divided between ICANN and privacy law and policy, and ICANN is a place where those two things collide, although up until I joined the board, I managed to dodge every single WHOIS review that has happened since we came here.

And I think many of you have said that we need the data protection authorities to be at the table in our discussions. I'm very happy that we have them here, and I very much appreciate

the sponsorship of the Council of Europe and the data protection authorities who are here with us to engage in dialogue.

As you heard, this is not going to be a once-and-done conversation. It's intended to reinvigorate and strengthen an open, inclusive, and not-nearly-endless dialogue on these issues.

So I'm going to briefly introduce the panelists. I have an initial round of questions. We will then move to questions from the floor and anybody who is participating remotely.

So first I'm going to start with somebody on the panel who needs no introduction and who is one of the sponsors of this panel, Thomas Schneider, the Chair of the GAC and the Deputy Head of the International Affairs Service and International Information Society Coordinator at the Swiss Federal Office of Communications. I had to read that because it's a really long description. I'm sorry.

So Thomas is here. He'll start off with a -- will ask some questions.

We also have Giovanni Buttarelli, the European Data Protection Supervisor. He was appointed to that job in -- by the European Parliament and Council for a five-year term in 2014. He had

worked in that office before, and prior to that, he was the Secretary-General to the Italian Data Protection Authority since 1997, which is almost since the beginning of time in this Internet privacy world.

Wilbert Tomesen is the Deputy Chairman of the Dutch Data Protection Commission and Vice Chair of the Article 29 Working Party. He reminded me today that the Article 29 Working Party first wrote to ICANN in 2004, and we've been in regular correspondence since that time. Joe Cannataci down there is the U.N. Special Rapporteur on the right to privacy. He heads up the Department of Information Policy and Governance at the University of Malta, as well as holding the Chair of European Information Policy and Technology within the Law Faculty of the University of Groningen. I hope I pronounced that right. He must live on an airplane because he also teaches. He's an adjunct professor at Edith Cowan University in Australia.

But all of you techies who are dreading a policy -- an endless policy discussion, take heart. He's a U.K. chartered information technology professor -- professional, I'm sorry, and fellow of the British Computer Society.

We also have Caroline Goemans-Dorny who is INTERPOL's data protection officer. In that capacity, she monitors INTERPOL's data processing compliance and works with the 190 data

protection officers designated in each of INTERPOL's 190 national central bureaus.

Finally, we have Gail Slater -- Caroline is over there and Gail is over there. Gail is Vice President of Legal and Regulatory Policy at the Internet Association. She has a career that's very close to my heart. Before that, before she joined the Internet Association in 2014, she spent more than a decade at the U.S. Federal Trade Commission, including a stint as Julie Brill's attorney-advisor, and I believe that the data protection experts on the panel will remember Julie as coming about as close to a data protection authority as we can get in the United States.

But I just have a word of warning to Michele who is out there. Gail is a dual citizen of Ireland and the U.S. and she holds a master's degree in European and comparative law from Oxford.

Finally, Jim Galvin, another who needs no introduction, has been on ISOC's -- on ICANN's Security and Stability Advisory Committee since its first year. He's been an active participant in the IETF for more than 20 years, and I was wondering, does that make you an active hummer?

And he is the Director of Strategic Relationships and Technical Standards at Afilias.

So we have a great panel here. We also know that there are some -- there's some expertise and perspectives in the audience that we particularly do want to hear from.

So let me start by asking a few introductory questions and I'm going to first turn to Mr. Buttarelli.

Giovanni, could you briefly give us a background on some of the fundamental privacy principles that serve as the foundation for data protection laws, including, but not limited to, the upcoming general data protection regulation?

GIOVANNI BUTTARELLI: Thank you, Becky, for your kind introduction and welcome to everybody.

My role is to act as icebreaker, and I will briefly start by saying that the principles I'm trying to shortly list are not only, I mean, European Union-based or contained in the Council of Europe Convention 108.

Increasingly, privacy and data protection are becoming global. A recent study has identified 120 countries in the world now equipped with the modern generation of privacy and data protection provisions. They are, I mean, largely departing from the system of self-regulation, and although some principles are named differently, such as, for instance, purpose limitation

principle, there is a lot of similarities, and supervisory authorities are cooperating around the world in a way which is increasingly growing.

I would like to ask you not to think that data protection is simply administrative burden and boring requirements as applied to Internet governance and to have a -- I mean, a short overview, you may have a look to the opinion I adopted in June 2014 published on the Web site of my institution where we tried to analyze what the European role could be in shaping the future of Internet governance in terms of democratic values, in terms of relationship with multistakeholders for the governance structure, and also with regard to the need for promoting a single and unfragmented network around the world.

Privacy is considered worldwide as a fundamental right, as an essential right, while data protection is recently considered as such in Europe and in a few other countries, but what is essential is that the protection of both privacy and data protection are considered by many laws in the world as a prerequisite for joining to benefit other fundamental rights and freedoms, all fundamental rights and freedoms, including, for instance, freedom of expression, the right to personal identity, and more recently, dignity. This is why my institution will host next year in Brussels the International Conference on Privacy

and Data Protection Commission to focus on the ethics of new technologies.

What about the principles in general terms?

We have, of course, transparency, which means clarity on who is doing what, and this is why the new definitions adopted, for instance -- not only, but for instance, in Europe about the role of a controller, of a processor, are key to, I mean, then identify a suitable framework in terms of accountability.

Lawfulness and fairness are then to be mentioned. And lawfulness does not only mean to have a legal ground to process the data, a contractor relationship, a legal obligation, a legitimate interest, consent, a vital interest of the controller of a third party but also consistency and compliance with all other relevant pieces of legislation, including those not related to data protection, such as, for instance, copyright, such as consumer -- consumer law.

Privacy by design and privacy by default are now, at least in Europe, new principles to be respected.

And the recent regional framework in the E.U. builds -- or more specifically aims at reinforcing data subject rights, at reinforcing supervisory powers of competent independent authorities, aims at modernizing existing data protection framework in having a

more coherent approach so that controllers should not fragment their policy depending on the territories.

We would like to have more accountable controllers. It means that data protection authorities should be more selective. It means that controllers should do more homeworks and identify a sustainable policy, have an answer to different problems, identify relevant risk, allocate responsibilities, demonstrated you comply with the law and you have a suitable policy.

This legal framework is to be applied to individuals, natural persons. And, therefore, the notion of personal data in the big data age is more than key. You have to identify also the impact on this legal framework on personal data relating to individuals acting on behalf of a legal entity such as a business company and a public administration.

I would come back in the second round on the purpose limation. But let me say 13 years after the ICANN event in Rome, we would like to come back to the questions we raised in the opinion we adopted in 2003 when in a nutshell we started making three questions to your community.

First of all, the first question was: Why an Internet domain registry is to be treated differently compared to telecom directories when an individual registers, for instance, a domain name? So the right not to be included in a register.

A second question, just to give you an example of how this principle then translate into practice was: Is there any other less intrusive method compared to mandatory publication that would serve the purpose of the WHOIS directories without being all data directly available online to everybody?

The third question related to bulk access for direct marketing issues.

We also tried to give you a suggestion with regard to access by third parties, law enforcement. And our assumption 13 years ago -- and the conclusion in my view is still valid -- was, let me quote in one second the relevant sentence, "The purpose of the WHOIS directories cannot be extended to other purposes just because they are considered desirable by some potential users of the directories. So this is, I mean, one example which may help in identifying what the purposes are. And we would like to serve you to make these principles effective in practice.

This is not an E.U. versus U.S. problem. This is a global dimension. It would serve in reinforcing trust and confidence in Internet. We are flexible enough to make this principle effective in practice. We would like to depart from formal requirements. We would like to focus on effective safeguards. And I think that all in all we are on the same side.

BECKY BURR: Thank you very much.

Wilbert, could you speak a little bit more about the accountability and purpose limitation principles? I think those are particularly important for our discussion.

WILBERT TOMESEN: Thank you, Becky. I will try to. And dangerous that I will double a little bit with Giovanni.

Allow me first to make a sort of confession because I have been a public prosecutor for over 20, 25 years. And I work as a supervisor in the data protection world since, say, about five years. And the combination of those two tasks means that you more or less think that you have seen everything and that you know everything. So I'm quite surprised by the size and the atmosphere here at this meeting, meaning that I'm very thankful and grateful for you to having invited me to participate here because this is an important event.

You should note over the years -- and Giovanni already told it -- European data protection authorities have closely been following discussions about ICANN, for instance, the public availability of the WHOIS data. We have participated in debates about privacy implication of the WHOIS. But this is as far as I

know the first time we meet face to face, and I'm really looking forward to discussion after our introductions.

Europeans, ladies and gentlemen, are granted by law the legitimate expectation that their personal data will only be processed for legitimate purposes and not be used further or kept any longer than strictly necessary for that purpose. That means that personal data shall be processed lawfully, fair, transparent. Those are basic principles laid down in -- already in our directive and in a year from now in the regulation in our European law, meaning basically that you should, we should, and controllers only should collect data for specified, explicit, legitimate purposes and should not process it any further than in a manner that is incompatible with those purposes, what we call the purpose limitation.

Secondly, an overarching principle, the data you process, by the way, also including making publicly available, should be adequate, relevant, and limited to what is necessary in relation to the purposes to which that data is processed. That's what we call data minimization.

So, basically, ladies and gentlemen, let's be fair, transparent, and, if I may say so, predictable.

A former colleague of mine in this context uses the word -- used to say "let's try for surprise minimization." Maybe that is what --

only yesterday we could read in the papers Tim Berners-Lee saying when he said, "I think we are about to lose control of our personal data." And as far as I'm concerned and as far as European data supervisors are concerned, being fair, transparent, predictable, working according to the law is one of the answers to that.

These are overarching principles and not negotiable principles. And I must say we, the data protection authorities, never get tired of pointing this out. And it also goes, I have to say, for the public availability of the WHOIS data.

Thinking of the principle, for instance, of purpose limitation, you know better than I do that the stronger purpose of the WHOIS is to make contact information available. But since then the WHOIS purposes have been expanded, public access, access to law enforcement, rights holders, security practitioners.

But the mere fact, ladies and gentlemen, that personal data are available in a register does not make it legitimate to use those data for other purposes just because, as we said before, it is useful. In order for ICANN, for you, to have a legal ground for publishing personal data, the publication must, indeed, be necessary, proportionate. And publication does not outweigh the privacy interest of users.

You should know that we at the DPA have received over the years a steady amount of complaints from people about the public availability of their personal contact details through the WHOIS. The data on many websites that, for instance, republish old WHOIS data available for practically everybody, for any purpose, good or bad.

Now, that should almost be my first remarks but allow me to have a last word because that goes to -- more to what drives me.

The predominant objective, ladies and gentlemen, of the new regulation, as I've said before, is fair, transparent, and predictable process of personal data of everybody in this part of the world.

Being accountable as controllers will mean to you being able to demonstrate your compliance towards us DPAs with those legal requirements. Again, the necessity of data processing, of data limitation, the way data subjects are informed about purposes and their rights will without any doubt be closely assessed in every country by every DPA in the E.U.

DPAs, by the way, by then granted with substantially penalizing powers. But, ladies and gentlemen, that's going to be my last words. At the same time I'm very misconvinced that organizations that hold full-heartedly the fundamental principle rules and by doing that -- the fundamental principle privacy

rules and by that earn trust and respect from their customers. I'm fully confident that those organizations will have the future. Thank you very much.

BECKY BURR: Thank you very much.

We'll turn to Professor Cannataci. Joe, could you -- third-party access to personal data is very much an issue for this organization in the context of WHOIS, for example, or in the context of some of the escrow data and the like. So could you talk a little bit about third-party access in particular.

JOSEPH CANNATACI: Yes, certainly, Becky. And, once again, I add my thanks to the organizers here for bringing together something which I think is long overdue.

And I think perhaps it would be best if we start by unpacking some of the things which have been said by Giovanni Buttarelli and other colleagues, which is to say that when we're talking about third-party access, we have to bear in mind the way that privacy and data protection law was born.

Actually, when you look at the way it was born in the United States and the early discussions between 1967 and 1973 and the

way it was born in Europe, it was pretty much made in a sense that if I give you data for one purpose, you're supposed to use that data only for that purpose or for a purpose, which is very compatible with that purpose. In other words, if you collect my data in the context of a banking situation to obtain a loan, you can only use the data for that particular purpose. And if you obtain it to get an insurance policy, that data should not be repurposed beyond that insurance policy, health data and so on and so forth.

So when we are talking about third-party access, I think we should bear in mind that this is the context in which we should be discussing it.

Secondly, I think we can see the way the things have changed in the way that if I go back to my own practice about 33 years ago in this field when I was thrown head-long into the discussion of protecting police data -- and we are fortunate here that we have Caroline as INTERPOL's data protection officer who CAN perhaps expand on that later. The same principle applies.

But if you look carefully at the first recommendations and regulations that the Council of Europe made, they were all built on the principle that the data controller is going to do most of the collection himself or herself, that the police force is going to collect most of the data itself, that the health company is going

to -- that the health provider is going to collect the data himself or herself.

Whereas in reality today, we have moved a considerable distance to the police or a health provider or a pharmaceutical provider, not necessarily collecting the data itself but depending on the data that somebody else has collected. Sometimes also data very often collected by private companies in a way where the citizen is often not aware of what is going on.

This is particularly important in a number of contexts because if you had to ask a number of companies operating on the Internet, they will tell you that they face tens of thousands of requests for access both to metadata and to content data.

And this not only comes in the law enforcement or intelligence context, although those are two very important contexts, because one company alone faces 17,000 requests and that provides -- provides a huge pressure, not only on the company but on the legal systems concerned. We don't have the time here to go into mutual legal assistance. But actually, if you had to be a prosecutor or an investigator, you could be faced with a legal procedure which you could go around it the old way, can last between 11 and 13 months on average for you to gain access to some data in some other country.

So third-party access is an incredibly complex thing. It's also becoming even more complex because of the fact that a number of governments, including European governments, the United States Government, the Australian government, the New Zealand government, a whole bunch of governments, have declared that something now is almost as holy as motherhood and apple pie and that's the principle of open data.

Now, 30 years ago when I started off in this business, we thought we had a safeguard for that. We thought that that's an anonymization or pseudo anonymization, which are two different things but we've moved on. And now when you use big data analytics to triangulate data from several sources and then you turn to open data, then you come to a point where you say oh, dear, perhaps this re-purposing of data was basically -- very often that's what you end up doing -- this re-purposing of data in a big data and open data environment means that you're giving third parties access in a way which has become a matter of a change in public policy.

And I think that these and many other subjects which are of direct relevance to third-party access are very important in an ICANN environment. Because in an ICANN environment, while ICANN helps provide the technological infrastructure to enable people to connect to each other, it must also eventually provide the way to implement certain policy decisions. And in this sense

the code is law. And I've got to remind you that when it comes to -- when it comes to third-party access, we must also remember it in the context of the legal infrastructure and the policies taken by all of those states, nearly, which Giovanni Buttarelli was referring to beforehand. When we have more than 102 -- between 102 and 120 states, most of which have followed the European model and the principles. That means that when they derogate from those principles, when they grant access to those principles, third-party access can only be granted as a rule, if it's for a specific purpose, in other words, protecting state security, public safety, the monetary interests of the state, or the suppression of criminal offenses. And when doing so it can't just be willy-nilly, but when doing so it must be done in the context where there is a law, it's provided for by law, and that law must provide appropriate safeguards.

So whatever discussions come out of this room and over the process that I look forward to ICANN having with people around the table and people outside the room, it's got to be taken forward in that spirit. In other words, that we've got to look at what people out there expect and what people out there expect are remedies. Businesses out there expect the ability to do business across the globe, and citizens out there expect to have their private data, their personal data, safeguarded across the globe and with safeguards which, as I like to repeat, if they can

go and operate and serve in an Internet without borders, they expect to have save guards without borders and remedies across borders. And I look forward to the discussion here in ICANN contributing to us identifying those remedies and also identifying where those safeguards can be technical safeguards, when they can be policy safeguards, when they can be legal safeguards, and the combination of all of those. Thank you.

BECKY BURR: Thank you very much. I think here we tend to think of law enforcement on one side of this debate and privacy advocates on another side of this debate and never the twain shall meet. I'm struck that Johannes's title is Director of Information Society and Action Against Crime and Wilbert was a prosecutor for many years. We also have Caroline Goemans-Dorny -- whose name I cannot pronounce very well, I apologize -- who is the data protection officer at Interpol, and I would love to hear a little bit more about how you work inside of law enforcement with respect -- on these issues.

CAROLINE GOEMANS-DORNY: Yeah, okay. Thanks very much for this question, and thank you for having invited me to this very interesting panel. As you may know, Interpol is the international police organization covering 190 member countries, and, in fact, the -- acts as an

international information hub for global police databases. So we indeed do process a lot of information.

If I can put it bluntly, very bluntly, perhaps Interpol would not exist anymore today if it hadn't put efforts and investment and put in practice the data privacy principles since 1982 already. And this brings me back, in fact, to the basics. Why are all these -- these principles? Well, it's to make effective police cooperation, we need trust, we need reputation, and we need to bridge gaps, especially when you are working in a global environment. And there strong privacy principles implemented in data protection standards come in and help us. They really play -- we have experienced at Interpol they really play the underlying framework on which -- on which effective police cooperation can then take place from police, from an operational, from a technical perspective. And it's, in fact, just like to take time to build strong foundations for a solid building.

So this long-term investment and belief in long-term added value of the data protection is a stand that Interpol has been taking since a long time, and as I said, it's not by accident that the first rules of Interpol on data protection dates from 1982 and that was just right after the adoption of the convention 108 of the Council of Europe on which it's based.

Now, over the years -- because that's not the end of the story. Over the years the privacy principles have been developed on and on and have really been developed in a sort of detailed code of 136 provisions. And we count 11 updates since 1982. So that's approximately an update of the standard data -- of the data protection standards every three years.

So data protection is really a dynamic process. The standards are only helpful if they're really flexible. And I think at Interpol it's a pretty -- it's really an asset to have rules that are flexible so that it can stay fit for purposes. And that's, of course, a continued challenge. Our latest update was in 19 -- of the rules were in 19 -- were in 2016, in November. And there the role of the supervisory body was reinforced, and already now we're working on a next -- or reflecting on our next updates, in particular on the -- on the cooperation with the private sector. Of course, there is a huge evolution, and the framework should be fit for purposes for that.

And that's -- leads me, in fact, to the second point about reputation. As mentioned earlier, it's not only about the -- the right of privacy or the fundamental rights are involved for effective policing. Also the right of freedom of expression. And Interpol's Constitution refers expressly to the Universal Declaration of Human Rights. It also states the organization principle of neutrality, which, in fact, means that the

organization cannot -- is prohibited from interfering in military, religious, political, and racial matters. And these -- these fundamental rules have been also reflected in all this data processing standards. And in this regard, I think that's the -- perhaps the added value of Interpol, that Interpol can act as a clearinghouse. There is a multi-disciplinary team of analysts, of lawyers, of police work, of police officers that work day and night with the night shifts to review the more than 3,000 requests per month received from member countries who are seeking Interpol's cooperation for the location or arrest of wanted persons.

So these requests are reviewed on the legality, on their quality, manually. Also with automated tools like, for instance, triggering on certain words. And also on the -- on the basis of specific criteria and thresholds. So this clearinghouse role is very important at Interpol to guarantee certain quality of the information and to make the police cooperation more effective.

Finally, the third and last point, I really believe that the strength of global privacy principles really lies in the fact that they have universal outreach and that they are bridging gaps. Gaps between the difference in legislation, in business processes, and that they create a sort of interoperability that makes things happen. Not only -- not only technical ones. These standards are really based on several pillars, effective implementation of

standards. It is all well to have standards, but if they are not known, not understood, and not applied they make no sense. So effective implementation, capabilities, training capacities, effective oversight, and redress for individuals. The standards at Interpol have been adopted by 190 member countries. Everybody finds itself in it. Once -- the cooperation via Interpol is a voluntary cooperation, but once you have chosen to cooperate the code rules are binding, there are corrective measures, there are sanctions that can be imposed.

And finally, I'll conclude by saying that, in fact, if we think about it, the privacy principles and the derived data protection principles are in fact just good governance principles. Why do you process? Purpose. What do you process? Accuracy. On what basis do you process? Legitimacy. How do you process? Transparency. How do you comply? Oversight mechanism. These are, in fact, all good governance principles and business organizations that have good governance principles have also good business. So that said, and I'll finish with that. I think we should -- we should, however, not get overexcited by legal standards only when we implement privacy principles. It's a process that's ongoing that's holistically -- it's about regulation, policy, business processes, the right technologies. It's, of course, very challenging.

And then finally, let us not forget a very important aspect, a component, and that's -- that has been already raised and that's ethics. Because that also pays off. Regulation says what can -- what you can do and what you cannot do, whilst ethics says what you should do and what you should not do and that's very important on the Internet. Thank you.

BECKY BURR: Thank you, Caroline.

Thomas, the GAC has been a participant at these endless discussions and dialogues, and I'd like to get your perspective on the GAC's thinking as we enter this new invigorated phase of dialogue.

THOMAS SCHNEIDER: Thank you, Becky, and welcome, everybody.

First of all, we would like to thank the Council of Europe for this initiative which we fully support and welcome because we think that it is very timely and relevant to have this discussion here and now in Copenhagen because we are more and more aware, as well, like everybody else, that data protection, privacy, but also data policy in a broader sense that goes beyond protection of privacy, is one of the key issues for our citizens, for businesses, for governments, for institutions, global institutions

that have functions like ICANN which are not necessarily with a privacy focus but privacy is more and more becoming an issue for everybody that is dealing with data when -- and everybody's now dealing with data.

So the key is that data is -- and the use of data is becoming the core resource for innovation, for economic innovation. It's becoming a tool that is allowing us to make our lives more comfortable, more secure, and this has a huge potential for innovation.

At the same time, of course, there are huge risks for abuse, for misuse of data, for losing control. People feel that they are losing control over their data. And so there are key challenges for us all that we are facing.

And one of the challenges, not just for us governments ourselves but also for citizens, and in particular for businesses, is that we have different jurisdictions with different regulations, different legislations, but also within a country, you have different parts of governments that have different functions. Ones are supposed to protect the human rights of their citizens, where others are supposed to go after criminals, and many times businesses are squeezed between these two, let's say, partners within the same government administration on a national level but also on more global levels.

And sometimes or many times we end up with conflicting expectations on businesses from governments, but as well also from consumers that on the one hand demand for data protection, privacy, on the other hand they demand for services where they can spread their data and information all over the world as easy as possible, and we do understand that for industry, for those who offer services, this is a particular challenge to know what to do with this.

And when Johannes Kleijssen said earlier that the Council of Europe is also turning into a multistakeholder institution, this is something that I can confirm after more than 10 years of representing my country in the Council of Europe. It is more and more including businesses, civil society, other experts, and one example, for instance, that I've been part of the elaboration as the chair of that expert group was, for instance, when the Council of Europe was developing human rights guidelines for ISPs in cooperation with the ISPs and of course in cooperation with civil society and human rights experts. And also there, the funny thing was that while we were doing this, we found out that in the same institution -- and that is also linked to Johannes' title -- the section dealing with cybercrime was working on law enforcement guidelines for ISPs, so -- and it took us some time to find out that this was happening in the silos, and once we found, of course we got together and we talked to them and

tried to make sure that these guidelines -- so the ISP industry in Europe would not conflict with each other and we actually had to eliminate some of the conflicts before we could issue them.

And so I think this is just one example on how important it is that people get together, break the silos, and also here I think it's the first time that data protection commissioners talk to the domain industry, other industries. It's probably something where the contacts have been more established and so we welcome very much that this dialogue is now extended as well to the domain industry from all around the world, and also that ICANN can learn more about how privacy regulation is done, is developed, is developing in different regions of the world, and that those in ICANN that develop frameworks for new gTLDs or other services where this is an issue can develop them, to the extent possible -- and we think it is possible -- in line with existing and like coming -- probably coming regulations, so that business actors and users are not forced to decide between which regulation or laws they want to break, the rules of ICANN or the rules of the country that they're operating in, which is something that has happened, of course, as we know in the past years.

And maybe I'll stop with a personal remark.

I think in my country where we also have a discussion about data policy and what is the future forward-looking data policy,

more and more people come to the conclusion that the notion of data protection in terms of prohibiting use of data may not be the most forward-looking way of implementing our rights that we have in terms of privacy because there are benefits, there are reasons why data should be used in order to solve problems, in order to make our lives better and maybe more comfortable, if that's an objective, but the issue is rather to maybe move towards less prohibiting data to be used but more control of the citizens, more self-determination that users can decide who is able to use their data, for what purpose, and so that we think about how to actually benefit from the potential that big data, Internet of Things and all of this is developing and we're trying to think along these lines in order to come up with a data policy that may actually be useful in the 21st century.

And this discussion this year is a part of the discussion and I hope that we'll have an interactive part where actually business people can come up with concrete issues that they have and talk about concrete cases. This discussion is good that it is happening here. It will continue, of course, on a number of other issues at the IGF, the Internet Governance Forum, of which we are happy to be the host this year, from 18 to 21 December this year in Geneva. Thank you.

BECKY BURR: Thank you, Thomas.

We are going to turn very shortly to interactive questions from the audience. We have two other sort of brief groundwork that we want to lay here.

Gail, businesses are going to -- are affected by any change in the content or availability of WHOIS data, and as we work towards making sure that we're all in compliance, what does business need out of this dialogue that we're embarking on?

ABIGAIL SLATER: Thanks so much, Becky.

Just to reintroduce myself, my name is Gail Slater and I come from the Internet Association. We're based in Washington, D.C. and we represent over 40 global Internet companies.

We have not been to ICANN since the IANA transition but we were, however, very proud to be part of that effort and, in particular, we were part of a group of 14 different organizations, including civil society, who filed an amicus brief down in Texas in support of NTIA, and thankfully we won, which was a good thing for the global Internet community.

So I'll try to be brief. I have three points to make and I think I have about three minutes because the most important thing is to get your perspectives today.

So from a business standpoint, I think it's really important to take a step back before we get into what businesses need, which is ultimately legal certainty, and talk about this in a very ICANN-specific context.

We are at ICANN. ICANN's foundation and mission is -- and I'm going to read here -- it's "to maintain the operational stability, reliability, security, global interoperability, resilience, and openness of the DNS." And I think there's a good argument to be made that the WHOIS database is key to that mission, and so when we talk about the privacy principles here, I think it's very important that we talk about it in a WHOIS context and in a context of what the Obama Administration used to be fond of calling "competing equities." And the competing equities when it comes to WHOIS -- and you don't need me to tell you this but just to give you the list -- we have trademark enforcement issues, we have privacy that's surely a very important equity, and we have other consumer protections at play preventing spam and fraud, we also have law enforcement. Some of them are aligned with privacy and then some are in different places versus privacy, but they are competing equities.

I think it's very important to remember that.

And I think it's also something that's been recognized from my research by the ICANN community, and I'll refer you to a report from the SSAC from 2012, and it was given a wonderfully descriptive title. It was called "WHOIS: Blind Man and an Elephant." And it harkens back to a Hindu parable, and the parable is that you have several blind men. They're all asked to go and compare the elephant. And they all touch a certain part of the elephant's body and they come back and they compare and they get into violent disagreement with one another as to what matters, what the elephant is, and what the elephant does and what it looks like. And I think that this is -- this is a very apt analogy as we talk about competing equities in the WHOIS context. It's also something I should note that has been recognized in European privacy law. Although privacy is a very important principle in the E.U. system, we do have from the E.U. court system an acknowledgment that privacy must ensure a fair balance between, on the one hand, observance of the fundamental right to privacy, and on the other, the interests of requiring free movement of personal data, which is important in this context, and it's very important for businesses that that balance be struck.

I will also note that the new European law which is going to come into force about 18 months from now recognizes this principle in Article 6.

Finally, I'll get to Point 3, which is the most responsive to Becky's question.

Businesses need legal certainty in this context, and right now, as I say, we have a system where we have competing equities. The principles are not settled. But businesses do need legal certainty, and if we're going to go with a global E.U. privacy regime, first of all, I'd ask the question: Is that the correct regime? Do we need to have a discussion about what the best policy for ICANN is in this context?

But if we go with that, I would flag that it's not clear and it's not been raised today whether it would apply to the entire WHOIS database or to the RDS that may come to pass soon enough.

For example, again from research, over 40% of the entries in the WHOIS database are, in fact, registered by legal persons as opposed to natural persons, and the E.U. privacy regime only applies to natural persons. So it's a very important distinction for businesses to know and understand whether or not that would apply in the ICANN context.

Another threshold question would be: What are the kinds of data that are implicated by a privacy norm that looks something like the E.U. regime in the WHOIS context?

In the E.U. system, we have a standard that applies to what's called personally identifiable information. These are things that can be linked or linkable back to an individual. When you look at the WHOIS database, much of it is technical information. It's not personal information. It's not sensitive personal information. Again, it would be very helpful for businesses to understand what exactly is captured by a privacy standard in the WHOIS context with regard to what information is in, what information is out, things of that nature.

So these are all important questions. I thank you very much for starting the dialogue today, and the GNSO, the business community, looks forward to continuing the dialogue.

BECKY BURR: Thank you, Gail. And last, but not least, our own Dr. Galvin.

Jim, the domain name industry is going to be directly affected by changing standards. What technical issues should we keep in mind and be aware of and thinking about as we have this dialogue?

JIM GALVIN: So thank you, Becky, for that question.

As I think about the principle of privacy by design and what it's going to take in this community to implement solutions and the solutions that are available to us in order to meet the needs of privacy by design, I find myself concerned about two issues.

The first one is data management.

We each, in the industry, have our own internal processes for collecting data from one location, copying that data to another location for storage, copying the data to another location for backups, copying it to yet another location for perhaps, you know, real-time hot standby of services, maybe yet another location for providing alternate services or additional ancillary services like reporting or directory services like WHOIS or the soon-to-be RDAP replacement for that.

And privacy is going to have an effect on what we can do there and when -- where this data can move to and how it can be moved. And we have to think about the burden that's involved in moving this data around and how we might have to change our own architectures or internal processes in order to meet those needs.

And some of those solutions will be more cost-effective than others and they will have a dramatic effect on what we can and cannot do and when we may or may not be able to do it.

So as we think about the policies that we're going to develop in order to meet these privacy requirements coming to us, we need to think about what we have to do on the back end to deal with our data as it moves from place to place and is stored in different locations.

So that's one. Data management.

The second question that I -- second concern that I have that I worry about is the access to the data.

In today's system, we have a relatively open system, right? Everyone gets access to all data at all times. That's essentially what the WHOIS system is that we have today in directory services.

The other end of the extreme, of course, would be no one gets any access to any data at any time.

But I think we can all appreciate that we are headed down a path to create a differentiated access system. We are going to have to create policies that define roles and decide who is going to be allowed to get access to things and how they're going to be -- go about doing that. We're essentially creating a credential

management system in which we're going to have to identify some set of people, provide them with some kind of credential, and there will be some other set of us who are then going to have to use those credentials in some way to validate that you are allowed access to a certain set of data.

So credential management systems vary significantly in their cost, from, you know, inexpensive to more expensive, and there are all kinds of failure modes that can happen in these kinds of systems, and there's, you know, much greater burdens associated with mitigating more of these failure threats along the way.

So, for example, to consider what these kinds of things mean, I offer to you the following kinds of things to think about that we have today in our community for credential management.

I mean, today we operate DNS infrastructures and we operate rather large infrastructures so we have a fairly substantial system -- many of us do -- that provides all-the-time real-time access to the data, so it's a hundred percent uptime and it's available to you. And so there's a pretty large investment in that kind of infrastructure.

In a credential management system, if you want your validation to work, I want to be able to access the data and know that if I give you a credential, I can get it, the presumption is there's

some kind of, you know, 100% uptime system that's going to let me validate that credential and know that it's there.

So that's something to think about. Is that really the path that we're headed down? And if not, who's going to be responsible for those failure modes? You know, what is our position going to be as a community? What kinds of policies do we want for dealing with those failure modes?

I offer to you another technology to think about, which many people will have some familiarity with. Think about our certification authority infrastructure that exists in the world.

We've all seen some fairly spectacular failures in that industry. You know, we have to think about our policies and what it means to us when we have those kinds of failures. How are we going to deal with those kinds of issues? Do we want to mitigate those kinds of failures or are we going to accept that they can happen and then what are we going to -- how are we going to apply to ourselves rules that allow us to accept them and deal with them after the fact as opposed to dealing with them in front?

So I think these are, you know, fairly substantial technology issues, one being data management and the second being data access, that we have to think about what kinds of solutions we're looking for, because what kinds of performance and

availability do we want to provide in order to meet the needs of privacy and where we want to go with that. Thank you.

BECKY BURR: Great, thank you. In the interest of time, we'll turn now to questions from the audience just so that there are -- there's a microphone right here in the middle, if anybody would like to ask a question.

As people are coming up, I think we've heard -- and I think this is irrespective of which privacy approach you take. We have heard that processing of personal data has to be legitimate and in order to meet the transparency standard, you have to articulate that legitimate purpose. The use has to be proportionate to the -- to the purpose, and it can't outweigh individual privacy rights. Let's try to wrestle with some of those pieces.

Joe, I just saw you had your hand up if you have a brief comment.

JOSEPH CANNATACI: Just a brief comment but one which highlight something said by other speakers.

Gail was referring constantly to E.U., E.U., E.U. Perhaps that can be understandable because it is the E.U. which has just finished the GDPR.

However, I think we should remember that the major treaty on data protection comes out from the other Europe, the Council of Europe. It's Convention 108. And Convention 108 is open for signature to countries across the world. Uruguay has signed it. Tunis has signed it. And other ten countries are now observers. And it is that convention which has actually provided the standard which more than another hundred countries around the world have followed.

And I'm saying that because I think it would be more correct. I don't wish to be too pedantic if we were refer to it as the European standard rather than the E.U. standard. That's not to say that the GDPR won't have an enormous impact. It will have an enormous impact because of some of its requirements and the references to -- for example, privacy by design, et cetera, will have an enormous impact worldwide. But most of the other principles are in common with the European standards which come out from Convention 108. Thank you.

BECKY BURR: Thank you very much.

Yes. And, everybody, please identify yourself when you speak.

LUTZ DONNERHACKE: Lutz Donnerhacke from EURALO. I have been part of the WHOIS review team once, and we had a discussion thick WHOIS or thin WHOIS. And I want to stress the fact that thick WHOIS implies that we had a worldwide, common, understood law system. So we do not have any problems with excess data or putting data in.

The thin WHOIS approach, on the other hand, distributes the data to the places where they are collected at the registrars. The only information we have in thin WHOIS is the information who is the next responsible party as we have in the WHOIS of IANA at the moment. If you ask a server of IANA for a special domain name, they say, I'm not responsible but we are contracted with the following registry. Ask there.

If you have a thin WHOIS approach, or ultra thin WHOIS approach, we get next response from the registry saying, Oh, we had sold it to the following registrar. Please ask there.

And if the registrar has the data collected directly from the end customer who can provide a WHOIS server in his local, lawful domain so that all the information WHOIS collected or given out never leaves the local place where this law is appliable.

So I urge you to think about if the thick WHOIS approach is the real, real correct way to do things. Thanks.

BECKY BURR: Thank you.

Without -- I just want to add one thought before you take this on. My understanding is that I can look up a name of -- a domain name of an European registrant in .COM, that will be a thick WHOIS -- a thin WHOIS. But I get access to the regular WHOIS data sitting at my desk in Washington. And my understanding of data protection law is, in fact, that's a transfer of data -- my ability to get that data sitting at my desk is likely a transfer of data out of Europe and subject to these standards.

So I'm not sure we eliminate the problem with a thick/thin distinction.

Any comments on that?

GIOVANNI BUTTARELLI: We're following at distance this debate thick versus thin data. But before giving you an advice, let me say that whereas the data protection community, frankly speaking, is still unclear what the purposes are.

And, therefore, I think before dealing with questions concerning the amount of data, centralized versus decentralized system, and access rights by -- I mean, on the basis of legitimate interests -- I'm not speaking now about law enforcement -- I think we should sit around the table and clarify what the purposes are. Because for us, frankly speaking, years after our opinion adopted in 2003, it's still unclear why this data has to be collected in that way, published in that way, so we would like to understand what the purpose is.

Is there any need to make identifiable a contact person? Do we really need to have an identified individual as a contact person? And are they properly informed about the publication of this data? Do you have a robust policy with regard to secondary purposes, particularly with regard to direct marketing?

I think if we first answer to this question, the rest will follow easily.

BECKY BURR: Thank you.

James and then I'm going to turn to Jim. Both of you have comments on this particular issue.

JAMES BLADEL: Just that taking up your suggestion that we gather around and discuss purposes. I know that this is actually one of the primary focuses of the policy development on RDS that we discussed earlier. I know it's been something that's also been a challenge of that particular working group, but it is good that we are -- to have that validated, that that work is part of the preliminary groundwork that needs to be completed in order to address some of these concerns.

JIM GALVIN: So -- and thank you. That's what I wanted to comment on, is to emphasize that when I was speaking about the fact that there are different solutions that we need to consider in this space of needing privacy requirements, you're highlighting the distinction between there are existing today two kind of solutions. There are thick WHOIS solutions and thin WHOIS solutions. And we really need to step back and think about which one of those may be more appropriate for providing our solutions going forward. And this is just a question that we need to revisit, all based on defining what our purpose is. Thank you.

BECKY BURR: Thanks.

Go ahead.

VITTORIO BERTOLA: Thank you. I'm Vittorio Bertola from Open-Xchange. And I have a couple of questions. But, first, I wanted to share my frustration because I have not been attending ICANN meetings in the last eight years, but I was an ICANN regular in the previous ten years when I was even a member of the board, the ALAC chair, and a number other things.

And it's really frustrating and depressing to see that I get back after eight years, and we are still at the same point that we were 15 years ago. Mr. Buttarelli was very kind --

[Applause]

He was very kind in remembering that, I mean, these questions were posed at the ICANN meeting in Rome, which was 14 years ago, 13 years ago. And ICANN still today has not been able to provide a convincing reason why this data needs to be gathered in the first place.

So -- and, also, I'm -- it's a little depressing that we're still hearing the same arguments. I mean, "This is privacy against law enforcement." It's not really privacy against law enforcement. The INTERPOL lady said it well. And I don't know of any criminal which would provide his true data when registering a domain name for doing crimes or whatever.

And it's not really about balancing a contractual obligation against a law because laws are more important than contractual obligations. Sorry. It's not like ICANN can impose people to steal -- I mean, registries go -- steal their customer's laptops, so they cannot impose registries to go and steal their customer's data.

So the question was in terms of -- for Mr. Buttarelli for the European authorities and the authorities of those 120 countries that have similar laws, is something really changing in terms of informed consent, especially in Europe as the GDRP comes into force?

So we've not really seen enforcement of the privacy law of the WHOIS in the last 15 years. And there's been a lot of patience, I would say, by these authorities. But sooner or later, there needs to be some real step to get the law applied.

So I was wondering whether something is going to change with the new GDRP, in any way there is an intention of doing this.

The other question is for ICANN. Though, I don't know who can actually reply to this. But in the case that -- I mean, the European data protection authorities sent a letter to all the European registries and registrars and told them that they have to stop collecting or publishing certain data, would really ICANN

suspend these registries or registrars? What would ICANN do? Because they are just abiding by the law. Thank you.

[Applause]

GIOVANNI BUTTARELLI: Vittorio, we are here today as problem solvers, not as problem seekers and not as enforcement bodies. Although all of us in 14 months will have to start with enforcement. And enforcement differently from 20 years ago is now based on serious fines.

So the question is how to prepare day one, which is 25th of May 2018. Why this is relevant for the rest of the world? Because the GDPR coming from a region will be applicable worldwide to everybody offering goods, in this case services, in the E.U. And, therefore, we will not take care of the servers, of the establishment, of the localization of certain services. What is essential is where the services are offered. How can we be able to help?

So I think when you build a house, you should start from what is strategic. In my view, what is strategic here is the purpose limitation principle, which is not only an E.U. principle, not only Convention 108. It appears in the OECD convention. It was in the White House draft Bill of Rights speaking about the reasonable expectation of the contents. You will find it in the

recent Japanese law. You will find it in the recent jurisprudence of the European Court of Human Rights. So it's a global and stable element, I mean, worldwide. It's a pillar which requires to specify the purpose.

We are not looking for extremely detailed purposes. But people are registering. People providing the data since the moment they provide the data should understand the context. So the purposes are to be specified. The purposes are to be explicit. It means sufficiently unambiguous. It means clearly -- I mean, expressed. And as data subject, me registering the data, me as the contact person, I have a right to understand in advance where my data will go.

The purpose is legitimate. We told you 15 years ago. So we are aware about the need to ensure a level of transparency.

But then we ask you, depending on the identification of the purposes, to understand with you the proportionality of the relevant modalities. And the two questions we submitted 13 years ago: Do you really need thick versus thin data to make this data publicly available in one shot? Is there a any different alternative to serve the purpose, to achieve all the objectives but in a more proportionate manner?

So I think this is extremely relevant. And if we have a problem of translation of principles, we can help you before we will have, I

mean, a living casebecause I'm sure right after May 2018 -- just because data protection authorities will become accountable for enforcing in these areas as well as in many others, it could be in June, September, December 2018. But it will come this day. And, therefore, we would like to serve you in advance.

BECKY BURR: Thanks.

Gail and Joe and Wilbert have responses to that. We're going to close the queue now so that we can get all the way through it because we are getting tight on time.

So, Gail.

ABIGAIL SLATER: Oh, thanks. Just a quick response. So, look, I think the reason why the debate has taken as long as it has is to go back to my earlier point about competing equities. I mean, I really think it depends on who you talk to within ICANN. And I think that they are equal equities. I don't see one equity that's trumping another within the ICANN system.

The only thing -- the only guiding principle is the bylaws, and the bylaws are about protecting the resiliency, the robustness of the DNS. I don't see any single equity plucked out from the queue in

the bylaws. So I think that's an important point worth making again.

With respect to WHOIS data and compliance with the upcoming GDPR and sanctions and fines and things of that nature, I will note that even within the E.U.'s own legal system -- and this is why, again, companies need some guidance here -- there is a competing obligation in the eCommerce directive, which is a directive that covers and creates obligations for all of my member companies. And those obligations are to disclose publicly data elements that look very, very similar to a WHOIS entry in that database. And so are we -- are we going to be in violation of the eCommerce directive? Are we going to be in violation of the GDPR? These are very important questions for businesses, and they are challenging. Again, there is a call for guidance.

BECKY BURR: Thank you. And if I could ask the responders to be brief, please.

Joe. No? Okay. Wilbert.

WILBERT TOMESEN: I try to be brief. I can echo what Giovanni has been saying.

You know what's important to me, when I talk to controllers, it's the very basic question: Why am I processing this data? Is it necessary and can it be done in an another less intrusive way? And if it comes to accountability, another principle of the new and upcoming European law, E.U. law, accountability only means for me convince me that you've been giving thoughts to those questions, the why, the purpose, the how am I securing your data. That's basically what we ask from controllers. Convince me that you have been doing your purpose.

For me, I have been enforcing my whole life approximately. So for me it's about compliance, and it's about being fair and transparent. And at the end of the day, yes, we will have to enforce. We can even be forced to enforce. But I would prefer data controllers to convince me that they ask themselves why am I doing this. And I'm doing this between all the proportionate -- all the modern principles that have been laid upon me. Thank you.

BECKY BURR: Thank you. And Vittorio. I know you are waiting for my answer. So the answer is at the end of the day, of course, you're right, ICANN cannot force registries and registrars to choose between their obligation to comply with applicable law and compliance with the contract.

Yes, go ahead.

MARIA FREDENSLUND: Thank you. My name is Maria Fredenslund. I'm director of the Danish Rights Alliance. We are a non-governmental organization working with I.P. crime here in Denmark. So we work with enforcement of crime, criminal activities related to I.P.-protected products every day. We also work with public awareness.

And what we see is that criminal activities -- I.P. products are increasingly used for criminals who use movies or literature to attract users in order to do other types of crime on these users' computers. So, for instance, a website which is often -- always registered in a foreign country is being used for attracting consumers, users, in order to install malware on their computers in order to do other types of economical cybercrimes.

So I.P. products are used as a way of gaining traffic to these websites.

And what we see -- what we saw last year was that -- and the Danish population is around 6 million people. We had last year more than 200 million visits to these types of illegal sites from Danish I.P. addresses. So that's a very, very huge number. And this is an increasing problem.

And one of the reasons why it's so easy to be criminal is that you are able to act anonymous on the Internet. So I can set up a website on a foreign domain name address, and I can be anonymous, and I can do my criminal activities from that side without the police or other to be able to do anything about these criminal activities. So that's a really, really big problem.

So, my point is that, of course, we need to be able to effectively enforce on the Internet, of course, with respect to the right balance between fundamental rights such as privacy and other principles. But for the moment, the thing is that it's very, very easy to be criminal. We do not have any way of interfering with criminal activities as it is today, not as a right holder, nor as a police authority. And one of the reasons for this is that it's so easy to be anonymous on the Internet.

Thank you.

BECKY BURR: Thank you.

GIOVANNI BUTTARELLI: I will speak for a second as a member of the judiciary, though attached to the data protection community and with regard to my background on criminal law, to say that I fully share your viewpoint and say that none of the data protection principles

prevent -- I mean, law enforcement authorities to have legitimate access, proportionate access to the data. And normally these provisions prevent the -- I mean, the WHOIS system to be easily accessible.

So one of the problems is also accuracy of the data. Accuracy is normally seen as a safeguard in the interest of the dataset. It is also relevant for entities having local access to the data.

So I'm encouraged by your comments. I don't see any big -- any big problem.

And if the problem is easy access through the world, this is the issue of international cooperation. And, once again, data protection principles are not the problem.

ELLIOT NOSS: Yes, hello, Elliot Noss from Tucows. We are a registrar and have been operating in this space since the dawn of ICANN. And I would like to start by saying that I am incredible heartened by this panel. This may be the most positive and optimistic panel that I've been in in the last five to ten years, that I can remember.

[Applause]

And that's because today at ICANN we have an imbalance, and that imbalance is such that we need you and your community to be more active. When I harken back to Thomas' comments about businesses being squeezed between competing interests, today at ICANN we are not being squeezed, we are being pushed from one side and that is today intellectual property and law enforcement. We would look forward to being squeezed.

I have two requests. The first is that for each of you that you become much more active. I am hoping that this panel is not a one-off. I am hoping that this is the beginning of a permanent place inside of the ICANN community for privacy folks such as yourselves. And I would urge you to -- for the benefit of every GAC member, to be present and to provide some equal pressure to where it is today for GAC members, where it's predominantly from law enforcement. Again, I don't begrudge either law enforcement or GAC members their current position, but they are not squeezed enough.

The second request that I have is that I think that ICANN needs to create a permanent privacy office, initially staffed with a privacy officer who's given real powers. And that's because the needs of this community are global. They take into consideration these national interests, but there are unique global elements to what we face, jurisdictionally in terms of the particular mechanisms and the particular approaches. And only

if ICANN takes that step will we truly be able to see safeguards across borders and remedies across borders. Thank you.

[Applause]

BECKY BURR: Thank you. I think we'll -- we'll take that under advisement. I think actually the GDPR may require us to have a privacy officer. Mathieu.

MATHIEU WEILL: Thank you very much, Becky, and thank you everyone on the panel. My name is Mathieu Weill. I'm the chief executive of AFNIC who is a ccTLD manager for France and also a back-end registry provider for a number of gTLDs in Europe.

So it's another industry perspective. I'm encouraged, like Elliot, and have a very -- I mean, I think the future is much brighter than it was. And my comment is actually a reaction to the statement that was given by James who's a very respected industry player in the whole world. But we -- as a ccTLD, we are obviously very concerned by this regulation. We take this very seriously and have been taking privacy seriously -- very seriously for years now. And I think the concerns that were shared by James are, if you look deep enough, largely overstated. It is not such a gap to be an industry player in the domain name industry and address

the various principles underlying the GDPR. And I think this is really important. We are open to discussions within the industry, within the GNSO. We have these discussions among European ccTLDs as well. There is sharing to be made to understand exactly the concerns from a practitioner point of view. It's not just the data protection authorities that need to help us. It starts with us, and looking at our processes and looking at exactly what that means to follow the principles of these regulations. And if you -- I mean, like Elliot, we support these principles. We live by them when we think about the Internet as one and respectful for individuals and uniting individuals.

And so I think we need to overcome the tendency to say well, it's a regulation that's been pushed on us so it's necessarily bad and it's good it's pushing us into the right direction. And there are challenges undeniably, especially for global players, but they can be overcome if we just put ourselves on the table, not fight against but try to find right solutions. Because those solutions have been around for a while. And we can find them. And I think the most urgent challenge that I'm going to urge ICANN again, like others, to streamline these processes, to help those registries and registrars who put themselves in compliance with the regulations that they are not held back by the various waiver or other processes from ICANN in order to comply. I think that's

the most urgent challenge along with cooperation, corroboration in the industry, to comply.

JAMES BLADEL: Thank you, Matthieu. Just to clarify, I think you meant James Galvin?

MATHIEU WEILL: Oh, yes, absolutely.

JAMES BLADEL: I think he would like to respond very quickly. Thanks.

JIM GALVIN: Yeah, thank you. I want to say that I agree with you. Not about being overstated but about the fact that the issue -- the solutions begin with us, that we as a community need to come to the table and have those discussions. My observation is more about we are creating a new system, the credential management system, and I assert -- and maybe, you know, we'll take this discussion offline and there will be more discussions, lots of time to deal with this -- that a credential management system is, on a global scale, is something that we've never been successful about in any industry. We do not have any globally scaled credential management system that deals with what's

required to validate identities, both just to deal with the credentials, having realtime access to validation of the credentials themselves, the operation of these kinds of things. That's my observation. So I think that as we move in that direction on that side, we have some real challenges here that none of us have ever really faced before in the large. So -- but I welcome that continued discussion on these issues.

MATHIEU WEILL: Thanks.

BECKY BURR: Thank you. So we have a public forum in here at 5:00. I'm going to ask the remainder of the people in the line to be as very brief as possible. We'll take all of your questions and then try to very quickly respond.

VICTORIA SHECKLER: Thank you. My name is Vicky Sheckler. I'm here on behalf of the RDS working group, and I have a two-part question for you which I'm going to read. Forgive me. With respect to the GDPR compliance by entities within the EU, would it be enough legally if ICANN consensus policies define a new RDS which allows for controlled access to registration data without requesting that the data subject's formal consent for each use -- for uses that are

lawful such as for the suppression of criminal or civil offenses? Alternatively, numerous stakeholders at ICANN have suggested that asking end users or beneficial registrants to consent to further uses of the registration data would solve the debate over the privacy of registration data made accessible through WHOIS such as for criminal or civil enforcement purposes.

What are your views on both of these using the PDP consensus process as defining the proportionality and the use of the data by third parties or using consent as the mechanism for legitimate proportionate lawful purposes. Thank you.

BECKY BURR: Thanks. So those are all very good questions. In the interest of time, I'm going to suggest we answer them offline. Keith.

KEITH DRAZEK: Thanks, Becky. Hi, everybody. Keith Drazek. I'm with VeriSign. I wasn't planning on asking a question today, but the earlier discussion around thin versus thick prompted me to get up. For those who have not followed it very closely, there was a thick WHOIS policy passed in 2014 that effectively is requiring VeriSign, for our .COM and .NET registries to go from thin to thick, to effectively collect data for 142 million domain name records from our registrars, the WHOIS data from our registrars.

Many of those are in the United States, but many are not. And in light of the new regulations, in light of the changed landscape since 2014 when the ICANN policy was passed, I'm curious if you have any thoughts about the implications of our registrars having to transfer in bulk records for 142 million domain names across jurisdictions? And particularly in the -- in looking ahead to 2018 with the new regulations and the possibility of a new RDS being implemented? And I'll just stop there, and happy to take that either now or later. Thank you.

BECKY BURR: Thank you. Also good questions, but probably a longer conversation than we can have here. Susan, did you want -- do you have?

SUSAN KAWAGUCHI: No, it was one of the questions (indiscernible).

BECKY BURR: This is not a once-and-done. This is the beginning of a dialogue. I would really like to thank the Council of Europe for bringing these incredible experts and expertise and resources in to this dialogue and thank you all for coming. And yes, Nigel, I'm going.

[Applause]

NIGEL HICKSON: Thank you very much, Becky, indeed. That was an excellent session, and we have to clear the room because we've got the public forum in nine minutes.

[END OF TRANSCRIPTION]