
ICANN71 | Virtual Policy Forum – At-Large Policy Session 3: GDPR as a Technology - Policy Implications
Tuesday, June 15, 2021 – 12:30 to 14:00 CEST

CHRISTOPEHR WILKINSON: Good morning, good afternoon, good evening, depending on where you are. I'm Christopher Wilkinson. I've been asked to launch this interesting session. I'm impressed that we already have nearly 70 participants. I'd like to welcome the participants. First of all, Joanna Kulesza will moderate the session and generally make sure that none of us take too much time in speaking because we want to reserve enough time at the end of the session for questions and answers and discussion.

Hadia Elminiawi is a very active member in the EPDP, together with Alan Greenberg and knows the subject pretty well backwards. Welcome, Hadia. Jan Janssen is an IP specialist dealing—and will address the question of technical implementation of GDPR by registries and registrars, given that apparently Verisign has obtained a patent specifically to do that. By the way, Verisign has apologized not to be present on this call but has offered to participate in subsequent discussions with At-Large and other interested parties.

And finally, Holly Raiche who is also a longstanding and very active member of At-Large will address the question of the future orientation and development of the work.

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

Very quickly in preparing for the discussion, I would just like to put on the table three questions. First is really, why has the EPDP taken so long? For some of us who've known for 20 years that there was a problem with ICANN's WHOIS system and European privacy law, one might have thought that some accommodation and possibly a solution would have been developed by now. I just don't understand—and I'm not a member of the EPDP group—why it's taking so long, particularly as there are some questions like the distinction between natural persons and legal persons which in other contexts are quite obvious and dealt with in the normal way in contracts and legal texts.

The second question relates to the proposed patent. The Internet has a very active, strong and longstanding technical standardization organization, it's called the IETF, and normally, one would have expected that if registries and registrars need a standardized implementation of a procedure or databases that the initial proposal would be a request for comments addressed to the IETF. And thus, I was surprised, personally, because it would be rather counterintuitive to have an American patent obtained by an American registry to implement what in practice is a piece of European legislation. So I wonder why IETF was not used in this case.

And the final point concerns the IDNs. My understanding is—and I'm not surprised—that implementing GDPR in the IDN context raises new and additional technical issues, and my understanding is that there is indeed a new working group being set up to address specifically that problem.

So I don't insist that all the panelists reply to all three questions, but if you run out of things to talk about, by all means, have a go at my questions. Thank you, and let's proceed with—well, first of all let Joanna take over completely as she's moderating the session, and welcome, and I look forward to a very useful and interesting discussion. Thank you.

JOANNA KULESZA:

Thank you very much, Christopher. Just a housekeeping note. I will inform our speakers of the time that is remaining. Each of the speakers has been allocated 15 minutes. Do use your time with the full amount that was allocated. But I do have flash cards, and I'll let you know as the time is running out. So these have different colors. I'm not sure you can see them. But I will appear briefly on the screen just to let you know that we're moving forward through our agenda. And without further ado, thank you so much, Hadia, for taking on the difficult challenge to give us a recap of the timely and challenging EPDP work. The floor is yours. Thank you very much.

HADIA ELMINIAWI:

Thank you so much, Joanna. I have a presentation. Thank you. So my name is Hadia Elminiawi. I'm one of the ALAC EPDP members. The other member is Alan Greenberg. I will be talking about the development of the registration data policy for gTLDs in light of the General Data Protection Regulation.

After the presentation, I will attempt to answer Christopher's questions, especially in relation to EPDP and how it is taking too much time. But I think the answer in the end would make more sense. Next slide, please.

I will quickly give you some background information, and then what phase one was about, and then I will talk about phase two, which is the standardized system for access and disclosure of data and its policy implication on end users. And then I will talk about phase 2A and where we are today. Next slide, please.

So as a quick background, the European Council adopted the GDPR in 2016 and it was put into effect on the 25th of May in 2018. ICANN substituted the noncompliant WHOIS with the temporary specification for gTLD, and this was adopted by the Board on the 25th of May in 2018.

Meanwhile, the community started putting together a policy in order to replace the temporary specification that needed to end in one year's time, so we needed to have a policy in one year from the adoption of the temporary specification.

In July 2019, phase one was concluded and phase two started, and that phase was [addressing] a standardized system for access and disclosure, and apparently, we are working on two remaining items. Next slide, please.

As I said, phase one started in July of 2018, and the outcome of phase one was actually very important, because it set the purposes for processing the data and thus the purposes for the collection of the data. So if we don't have a purpose for the collection of the data—and we're

not talking here about the display or publish or disclosure, it's just the collection—we cannot actually collect it.

So phase one actually determined the purposes for the processing of the data, and then based on these purposes, the collected data elements were determined as well as the transfer and retention and the data elements also definitely that need to be transferred and also the retention period. This was determined based on the purposes, and then also, phase one determined which data elements can actually be displayed in the public RDDS and which data needs to be redacted. It also adopted the temporary specification as an interim policy. Two recommendations were not adopted, and we'll talk about them in the following slide. Next slide, please.

We had some topics deferred from phase one which is the display of information of affiliated versus accredited privacy proxy providers, the redaction of the city field, the retention period, ICANN purpose number two which I will speak about later, and then also if the office of the chief technology officer needs a specific purpose, accuracy, differentiation between the data of legal and natural persons—and the reason this was raised is that the General Data Protection Regulation actually applies to the data of natural persons and not that of legal persons—and the feasibility of unique contacts to have a uniform anonymized e-mail address, and this was put forward because of the need of an address in order to contact the registrant in case of domain abuse or other necessary reasons, technical failures for example. Next slide, please.

So phase two started on the 4th of March in 2019 and concluded in July 2020, and it basically addressed two topics. First, a standardized system for access and disclosure of the data, and the second were the priority two items that those are actually the items that were deferred from phase one. So actually, phase one set the stage for us and phase two is speaking on how to disclose the data elements that were determined already in phase one. Next slide, please.

Those are the priority two items I mentioned before. Next slide, please. So phase two, we had the deferred items, and it concluded most of them apart from two, so it concluded that the information of affiliated as well as accredited privacy proxy providers would be displayed. The city field is not a must to redact, so contracted parties can leave it. And just to note, the city field is not actually personal information per definition. And it determined the data retention period as 18 months and it added ICANN purpose to contribute to the maintenance of the security, stability and resiliency of the domain name system in accordance with ICANN's mission. That purpose is in line with an advice received from the European Data Protection Board. Because of that purpose, there was no need to have a special purpose for OCTO. And then in relation to accuracy, it was decided that a scoping team would work on that.

What remained from this phase was the distinction between legal and natural persons' data, and again, to note that the data of legal persons is not actually protected under GDPR. Of course, personal information cannot be published anyway whether it is a legal or a natural person. And the feasibility of unique contact. Next slide, please.

So the next slide actually explains what the standardized system for access and disclosure is about. A requestor or a system user—and that is typically the requestor—needs first to be accredited by an accreditation authority. That accreditation authority could be ICANN or a third party determined by ICANN. And then the requestor also will need to have credentials. For that, we have an identity provider. The identity provider would verify the identity of the user and provide credentials to the users. The credential of the user is accompanied with some assertions. Those assertions are related to the role of the user.

For example, if the user is an intellectual property practitioner, he would have some assertions associated to his credentials. If it's law enforcement agency, it'll also [inaudible] and if it's another entity, it will have different assertions associated with its credentials. So the user now has credentials and is accredited by an accreditation authority, and it will go now with these credentials to the central gateway manager—the central gateway manager is typically ICANN—and would submit a request. And then ICANN or the central gateway manager would look into the request and then if it's a full request that satisfies the criteria and includes all the requirements, the central gateway manager would direct it to the relevant registrar.

So the system as such looks like a good one. So all users of the SSAD need to be accredited. Anyone can be accredited. It standardizes the request, the criteria and the content. It specifies response requirements. It determines the required service level agreements. It sets principles for logging and auditing and reporting. But the problem here is actually in the details in there. Next slide, please.

So, what is the implication of such a system on end users? Such a system actually does not change the current status quo. So if we look, for example, at the SLA requirements, for an urgent request—and this is considered a priority one request—this would take one business day in order to receive an answer and not to exceed three calendar days. That means if you submit a request on a Friday, you can get the answer on the following Monday. And by urgent request, we are talking about requests that pose an imminent threat to life, serious bodily injury, critical infrastructure, or child exploitation. And for that, you can actually get the response three days later.

So let's look at other actions like for example phishing, malware and fraud. These are considered priority three items, so the response would typically take three business days. Of course, it can take up to five if you're going through a weekend. Again, [that does not] provide the necessary protection for customers. For example, end users cannot independently verify the legitimacy of a website providing services, and this is because the data of the legal persons is not published. The system does not really support automation, so manual reviews are expected, and if you talk about manual in the Internet era, it means instantly hindering everything.

So the system was supposed to provide some kind of automation, but we ended up with only very limited cases, like I would say there are four, but one of them for example is city field, if it is redacted then it can actually be disclosed automatically. Another one is in relation to the—so again, the system as such, [the structure] and how it looks like, it looks like a good one, but the outcome of the system does not change

anything for end users. I would say it is a free pass to delay requests in relation to imminent threat to life or serious bodily injury to up to three days, and maybe before, it could have been handled earlier than that.

In order to answer quickly Christopher's question in relation to the EPDP, I would say that phase one—and that one was very important because it actually allowed the registrars to collect the data and it also determined the data elements to be collected and [those—under] the data elements that are going to be displayed and redacted. So this phase was very important, and that one concluded in one year's time.

So I would say the EPDP, the expedited process, did serve us here. However, it is still lingering because of—so having phases was actually a good thing. Phase two as we see did conclude some of the deferred items, which is a good thing, however, the system proposed as it is does not provide the requirements for end users. If we could quickly go to the second slide.

So I'm done. I would just say that phase 2A is just tackling two issues, the first of which is legal versus natural, and I think this is important, again, for end users. Thank you so much for listening, and I'm happy to answer any questions.

JOANNA KULESZA:

Thank you very much, Hadia, for your understanding with me trying to be a very strict timekeeper here. We are taking note of the questions. Thank you, everyone, for putting these in the chat. We will leave an allocated time space for the Q&A session. This is why I'm being so strict

with the timing. The questions are being taken note of. Please kindly follow instructions from staff when it comes to the format. Thank you to these who are following this standardized way we interact here within the meetings. If you could indicate who your question is aimed at, that would also be helpful, but we will do our best to collect these and address them as we progress.

Again, for the purpose of staying on our agenda, I will swiftly give the floor to Jan. Thank you, Jan, for agreeing to talk to us here today. The Verisign patent looks promising, but we cannot make heads and tails out of it without an IP lawyer. So, thank you very much for taking the time to try and explain this. I will pop into your window again with those little flash cards giving you a time check, but do feel free to dispose of the next 15 minutes. Thank you very much.

JAN JANNSEN:

Thank you, Joanna, and thank you all for this invitation. As Christopher said during the introduction, Verisign was recently granted its US patent application, and it's a patent application for systems and methods for preserving privacy of a registrant in a domain name system.

What does it mean? What can Verisign do with it? How will this patent impact the DNS and the current discussions that exist about Thick WHOIS, the registration data access protocol better known by this community under its acronym, RDAP, and the proposed standardized system for access and disclosure that Hadia was talking about, also better known under the acronym SSAD?

Before we engage in a discussion on these topics, I should mention to you that I am a Brussel-based lawyer that's qualified to practice in the EU, and while I do specialize in arbitration and dispute resolution with a particular focus on IP, [IT,] privacy, competition and Internet governance, I am not a US-qualified lawyer. So anything that I'm saying here between these walls should not be interpreted as a legal advice whatsoever.

During the next 14 minutes, we will focus first on some basics of patent law, taking a global perspective. Secondly, we will briefly touch upon the territorial reach of patent protection and geographic differences that exist across jurisdictions, to then focus on the family of Verisign patents that are at issue, namely those patents for systems and methods for preserving privacy of a registrant in a DNS. And then finally, we will come back to the questions that I already introduced.

So first, some basics about patent. The first question that we should examine is, what is a patent, actually? A patent is a grant of a monopoly right to an inventor. It is the inventor who decides who may use the invention in commerce and under what circumstances the invention may be used.

The Verisign patent that we are examining here is a patent that is a so-called utility patent, and that is a patent that may be granted to anyone who invests or discovers any new and useful process, machine, article of manufacture or composition of matter, or any new and useful improvement of such process, machine, article of manufacture, etc.

Who can obtain the patent? Well, the first inventor can, or the assignee of that inventor. In this case, Verisign. There are several conditions to obtain a patent. There is the subject matter of the invention. The subject matter must be allowed for patent protection. And to give you an example of something that is not allowed to be patent protected in the US are certain inventions in the atomic weapons industry. They are excluded from patenting. But that's not at issue here, obviously.

Processes and methods are allowed for patent protection, and in the US, US patent law defines process as a process, act or method and primarily includes industrial or technical processes. A similar approach exists in the EU and other parts of the world who accept processes to be patented.

And then the US current first inventor to file provisions provide that patent may not be obtained if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains. That's quite a long text, but there are basically two requirements that can be derived from it. It must be new, so it must be different from what previously existed—what is called prior art through a technical term—and the differences to that prior art, they may not be obvious. It's the non-obvious standard that is used in the US. In the EU, there is a similar requirement which we call inventive step.

So those are basically the main conditions for a patent to be protected. So the subject matter must be patentable, it must be new, and there is that non-obvious criterion, or the inventive step, which must be present.

Then there is the extent of the protection that is offered by the patents, or in other words, territorial reach. territorial reach is limited to the jurisdiction in which the patent is granted. So a US patent is enforceable in the US only. It is possible to apply for the same or a similar patent across multiple jurisdictions to obtain more global protection for the invention, and there are treaties in place to facilitate that patent application process across multiple jurisdictions.

But there are some differences that exist between jurisdictions. For example, with respect to subject matter that is patentable. And there are quite some differences in the patentability of what is called software-enabled inventions across jurisdictions. And why do I mention software-enabled inventions? Because the patent that Verisign was granted is based on a software and hardware solution.

Now, allow me to first focus on the jurisdiction that I practice in, and that is in the EU, you have articles 52 c and 3 of the European patent convention, and those state that the computer program claimed as such is excluded from patentability. But computer programs are not excluded from patentability under all circumstances, according to jurisprudence.

A computer program product which comprises all the features of a patentable method so that it enables a computer to act as an

apparatus, as a tool to carry out the patentable methods may be patented. A computer program is [thus not occluded] from patentability if the program, when that program is run on a computer or loaded into a computer, when that program brings about or is capable of bringing about a technical effect which goes beyond the normal physical interaction between the program, the software, and the computer on which it is run. That is what the case law standard says.

So the software and the hardware that is described in the patent claims must carry out a method or process which in itself is patentable. So under that standard, if we were to look at the Verisign patent, they are describing a method in a correct way to be protected under EU law.

In Japan, the situation is much easier because Japan explicitly refers to computer programs as patentable subject matter. Finally, the US, their patent protection for software-related inventions on recordable media is allowed but not the computer programs themselves. So if the software-related invention can be recorded on a medium, then it can be protected.

Then turning back to Verisign's patent now that we established a bit of the technical framework, we observe that it was very recently granted in the US. There was also a corresponding patent application in the EU, but this application is deemed to be withdrawn after the European Patent Office, the EPO, provided its initial search report. So, what does the EPO do? It is going to look at what prior art is there to determine whether the patent is new, and it will also give its opinion on the inventive step—in the US, the non-obvious criteria.

The EPO found that the patent claims in that corresponding patent application lacked novelty or represented common design options belong to general common knowledge of data authentication and DNS registration procedures.

But these findings of this initial search report were based on a previous European patent that was granted to Verisign and which contains many similarities with Verisign's US patent that we are talking about today. Because of this situation, you will observe that there are subtle differences between jurisdictions in the way that protection is offered to Verisign's patented systems and methods for preserving privacy of a registrant in a domain name system.

The previous European patent of Verisign has lapsed in quite a number of contracting states, including in Belgium, Luxemburg, France and Ireland. The patent remains valid in the UK and Germany for instance.

The Verisign patent, what does it describe, actually? It describes a data flow management with use of encryption technology. And this data flow management is something that typically happens across jurisdictions and on different services across the world. So this fact that it is really in an international environment could create additional burdens in trying to have this patent enforced when Verisign sees that its invention is used by different providers.

And a question that we ought to ask ourselves is, how will the ubiquitous nature of the DNS be impacted by Verisign's national patent that must be and might be enforced locally? And really, I think the key question for the Internet community is, what will Verisign's

enforcement strategy look like if we develop systems to protect privacy while preserving other important interests of the Internet community?

The patent actually describes sort of a privacy by design solution for managing personally identifiable information in the registration of domain name. A question that many may have is how inventive the described method is actually. Some may wonder whether the solutions where you're using encryption technology to anonymize or pseudonymize the ID of a registrant and that you use a third-party service provider for that, that the solutions are rather obvious. Future may tell.

Another important question is, will Verisign be invoking its patent in policy discussions? When certain structures to protect our managed data are being discussed, for instance in the implementation of SSAD, how will Verisign look at this? Will it say, "I'm sorry but the solution that you are describing there falls under the patent claims we have under our US patent and potentially the previous European patent as well?"

So these are really questions that we have as a result of this patent, and I think it's a pity that Verisign is currently not in the room, because if there's anyone who has the answers to that, it is Verisign. But I think these are questions that ought to be debated, and I will leave my time for debate because I think that will be the more interesting part of this discussion today. Thank you.

JOANNA KULESZA:

Thank you, Jan. That was incredibly helpful. Thank you so much. This is exactly what we were looking for. Just to wrap up, we have a US-based patent that works in some European countries, might work in other countries, and as you just rightfully noted, Verisign could raise it within ICANN policy development debates.

Now, as Christopher noted, Verisign is open to following up on this discussion, but for us to be able to ask the right questions, we needed to start off with this discussion today. So thank you again, Jan, for agreeing to join us and shed some light on a technology, as Hadia explained, specific enough to be granted a patent on whereas there is a discussion on how this patent might be implemented. And that is a question I have no answer to, but I'm certain Holly does. And with that, I hand the floor to our next speaker. Thank you again, Jan. Holly, the floor is yours.

HOLLY RAICHE

Thank you, Joanna. And actually, I don't have an answer. I think that is a fabulous question, but I am taking a different tact. And when we say intellectual property implications for further work, I'm actually raising another type of intellectual property for the question. And it's raised by the GDPR and it's also raised by the EPDP in the second report that Hadia talked to. Next slide, please.

My very brief talk will be about trademarks and about what happens in an environment of post-GDPR, because pre-GDPR, there was ready access to WHOIS data and that meant if you had queries, including

about trademarks, you knew exactly where to go and it wasn't a problem.

What GDPR has raised is who's going to get access to that data in what circumstances, and that's kind of a—yes, it's a little bit of a tale onto what [we just discussed] about, but it's a separate question, and trademarks and trademark law, although they're normally—you think about trademark and the intellectual property community, there are implications for end users, including small business.

So just to start with basic IP law, what's a trademark? And of course, [inaudible] have lots of things to say about it, but there are some standard words, some kind of sign, expression that identifies the product or service that you're talking about. And its value may often be because the trademark says something about the quality or nature of the product. Its importance is commercial, both as an identifier and possibly as a designator of qualities which you're looking for.

So trademarks are most often thought of and recognized in a commercial context, and I'll just put a few of the typical trademarks. Obviously, it can be a product or it can be, let's say, the Internet products, a service. Next slide, please.

First of all, how do you acquire a trademark? And you acquire it by using it. It could be a brand name, something you use in advertising or whatever, in relation to what you're offering, what goods or service. And you use it to the extent that is recognizable in a business context and in the context of a way of differentiating that from something else. Even if you don't register it, under common law—that's American/UK law—you

can nevertheless enforce a right as long as you can establish the elements.

In Australia, we have consumer law and it would include the phrase misleading or deceptive conduct. So if somebody is misusing a trademark, there may be an action that what they're doing is misleading customer into thinking a product is another product or another service.

If you want to register the trademark—and most large businesses will—there are tests for the registration, very similar to what—you acquire trademark by use. Usually, they're spelled out in national legislation. They use terms like you acquire it through use, you use it as a way to distinguish your product or service from something else, and it's in the course of trade. And generally, those are the sorts of things that you must establish to get registration.

And then once you acquire registration, generally, it's enforceable in the courts, and generally, once something is trademarked, it is recognized under a number of international conventions. And I won't name them at this stage.

Why are we talking about trademarks now? And since particularly ALAC is for end users. I would have to say, after COVID-19, any business that is going to survive will have trademarks and some of them might be in the nature of a domain name. Next slide, please.

And we'll talk about domain name as trademark. The first question, is a domain name a trademark? Well, not necessarily, but you can use it

that way. And if you use it that way, in the ways that I've described about use in connection with services, recognizable, etc., and it's a way to distinguish your good or service from something else, then arguably, it could be a trademark.

The interesting possible way of thinking about trademarks and enforcement is a thing called cybersquatting, which in some jurisdictions is illegal, and that's when somebody buys a domain name and tries to sell it back to the person that had the domain name or has the name, [which is, by the way,] in case you've heard of it, it's not really relevant in this discussion. Essentially, once a trademark is established, whether or not it's registered, it's yours to use. Next slide, please.

How do you enforce a trademark in the context of the post-GDPR world? Now, pre-GDPR, it's very clear that if there was someone who was using your trademark, including perhaps a domain name if it could be established the domain name could be used as a trademark, then you could obtain the necessary details from WHOIS and contact that individual, the alleged offender, and then take action under trademark law, possibly common law or consumer law.

What does that look like in a post-GDPR world where we know that that kind of contact information is not necessarily available to all? So in terms of this session, the intellectual property post-GDPR is all about who can access and to what extent can they access the information. Next slide, please.

So, if you have a trademark including a domain name used as a trademark, and someone—a company, an individual—has abused your

trademark domain name, and you need the information, you have to ask, okay, where's the information and how do I get it? Am I eligible? Can it be refused, and can I appeal?

Now, the answers—and I want to qualify, when I say answers, come out of the final report of the temporary specification for generic top-level domain registration data phase two, which has just come out, so my answers must be qualified because that report still—although it says final—has some ways to go and it's not clear that those are the final rules. So I can only guess that the next couple of slides will have the answers, but I'm not sure, because I'm not sure of the final report being a final final report, if I can put it that way. Next slide, please.

Okay, where is the information? Right now, the information is held by the registrars and the registries with thick WHOIS. But we know in the future, what is planned is that the registries will all be thick and they will all hold the data. Now, earlier, even months ago or a year ago, you would have said, "Well, will everyone hold all of the data that used to be there?" I think [inaudible] has answered that to some extent, that contact information will actually be gathered, so it's not a matter of has the information been gathered, I think. Again, all this is qualified. But it will be held. And how do you get at it? Next slide, please.

Okay, now we have to talk about—and this is assuming that in fact the relevant registry is thick and holds all the data, and we're assuming there's a thing called central gateway manager that is talked about in the phase two final report. Reading through that report, your first question, is the complainant an accredited organization or individual?

Apparently—and this was me reading through the report—both legal and natural persons may be eligible. And I'm just noting the paragraphs I was reading. Paragraph 1.4.2 suggests that an individual may make a legal request with a legal basis for the request amongst requestors—an example is for what they call the trademark ownership or registration, which suggests to me, if your complaint is about trademarks, that you may have access rights.

Further on in that report, it says additional information can include information asserting trademark ownership, which cemented for me the thought that trademarks and your claim for trademarks which might include domain names will possibly give you an access.

And finally, in paragraph 7.1, it includes intellectual property infringement, and consumer protection. As I've noted, both of those actions can be used to enforce trademark rights. Next slide, please.

The next question, can the access be refused? And if it can, can you appeal? Well, there are some qualifications here. Under—to report, it says central gateway manager may recommend, which suggests that he or she may not.

Next, the contracted party may follow the central gateway manager's recommendations, or they may not. But if they do not, they must give reasons. And it seems that the complaint can, if access is refused, go to ICANN Org. I'm not sure what ICANN Org is going to do about it, but apparently, they might be able to do something about it.

And the final from paragraph 8.5, absent any legal requirements, disclosure cannot be refused solely for the lack of the following, which would be court order, subpoena, court action or UDRP or URS.

So it looks as if under the structure which is being proposed by part two, you may, if you have a trademark and in that you include a domain name, and it meets the tests for domain name as a trademark, you may be able, using basic intellectual property principles and what's in the second phase report, you may have an action, but I can't promise that. Next slide, please.

Thank you. Questions? And thank you. And Joanna, see, I'm in time.

JOANNA KULESZA:

Great job. Thank you very much, Holly. We do have a few questions in the chat, and staff were wonderful in following the chat. I know they have taken note of these. The first questions are aimed at Hadia. So we're going to move into the Q&A session. We will start with the questions that were posed in the chat. I'm going to ask our wonderful staff support team to read out the first, I think, two questions coming from John for Hadia. There are, I believe, two more questions or issues raised in the chat, so I'm going to give the floor to Michelle.

Do feel free to pose your questions in the chat as we progress. Time permitting, this format, as opposed to a webinar, allows us to share [comments live,] so time permitting, if there are any comments or questions to be asked live, I would love for that to happen. But let's start with the questions in the chat as we have them. Michelle, if you could

read out the first two questions for Hadia. I would give the floor to Hadia to try and respond, and we'll try to proceed as indicted. Thank you.

MICHELLE DESMYTER: Thank you, Joanna. Our first question comes from John McCormick. Does it have the inhouse expertise to run this kind of operation? Please go ahead, Hadia.

HADIA ELMINIAWI: Thank you for your question, John. I cannot speak for ICANN to say if they have the expertise or not, but I assume John is talking about ICANN being a central gateway manager, because we already said that the accreditation authority can either be ICANN or ICANN can actually give this to a third party as well, of course, as the privacy provider that also could be a third party.

Central gateway, yes, it has determined to be ICANN. I guess if ICANN cannot do that, then it could also delegate it to a third party. But then I cannot answer if ICANN can do it or not.

JOANNA KULESZA: Thank you, Hadia. If we could proceed with the questions, Michelle, that would be wonderful. I believe there are a few more that were presented during Hadia's intervention. She might want to reply. If any other panelist wishes to chime in, feel free to do so. Thank you.

MICHELLE DESMYTER: Thank you, Joanna. Our next question is from Dmytro Kohmanyuk. The question is, what is wrong with regular Q&A window, and are we using HTML or XML?

HADIA ELMINIAWI: And I assume that he is talking about queries to the RDDS, that's correct? But how would you provide the authentication required and all that stuff? Because remember that the disclosure of the data needs to be for lawful bases and legitimate interests. And how will you be able to provide this? So it's not how you actually display it but how you verify actually the lawful basis and the legitimate interest based on which you would actually disclose the data. Remember, all the data that's not public is not public because it is personal data under GDPR.

JOANNA KULESZA: Thank you, Hadia. I believe that this was more a question on process where Dmytro was trying to find a dedicated slot for questions during our session, and as Jonathan notes, I believe the webinar format we have chosen is somewhat more interactive. But thank you for that reply. That is very helpful. And we have two more questions for Hadia. Michelle, maybe we can take these in bulk and we can proceed with the discussion. Thank you.

MICHELLE DESMYTER: Thank you. Next question is from Reg Levy. "What is fraud considered to be in this context?"

HADIA ELMINIAWI: I will quickly think of COVID, the pandemic and all those sites that were taken down because of the healthcare fraud that came with the pandemic. So when we are talking about end users and fraud, this is the kind of fraud we're talking about. Thank you.

MICHELLE DESMYTER: Thank you. Our final question comes from Chokri Ben Romdhane. "What will be the role of ICANN community in the SSAD implementation phase, and who ICANN will manage to collect necessary implementation funding?"

HADIA ELMINIAWI: So usually with ICANN, there's an Implementation Review Team that any member who's interested in actually being part of can submit a request and join the implementation team. So there is the Implementation Review Team for phase one, and for any policy, this is like the process.

As for who will bear the cost, first you need to make a cost-benefit analysis before you start implementing such a system, and based on this cost-benefit analysis, I think, this is where you would decide who pays for what. But I assume—well, I wouldn't like to get into the financial details there, but financial aspects are one of the things that would be—because I did mention that there's supposed to be a standing committee that would deal with elements related to the SSAD

that are not clear at this point. And many of the financial aspects actually belong to this, and so yeah. Thank you.

JOANNA KULESZA: Thank you very much, Hadia. I see there's one more question that just popped up from Emma Caner. I'm going to try to read that out. Let me know if have anything specific you'd like to add. The question reads, "When do you think we'll have an implementation date for the SSAD?"

HADIA ELMINIAWI: I'm not sure yet. We're not sure if SSAD is going to be implemented at all or not. So first, it needs to be adopted by the Board, and then the implementation phase would start. So to begin with, I'm not sure if it will be implemented.

JOANNA KULESZA: Thank you very much. I believe that concludes our list of questions, at least the ones that I have noted down. What I would like to do now is let our panelists—Hadia, Holly and Jan—add anything to what has been said before. Maybe you might want to react to the issues that were raised. It seems as if three years on from the implementation of the GDPR—which caught the ICANN community by somewhat of a surprise—we are still trying to find the appropriate way to accommodate to these European policy requirements.

We've looked at three possible models, I believe. Hadia giving us a very thorough recap of the work the EPDP has done, there seems to be an

opportunity to look at GDPR, being as specific as it is, through a patent application, something that Verisign has done successfully. Holly indicated the trademark policy implications. And those of you who joined us yesterday for the plenary also heard about the Council of Europe plans to reintroduce WHOIS through an additional protocol to an international treaty.

So I would love to hear from our panelists if they have any thoughts they would be willing to share, and then benefiting from the Zoom room format that we have adopted, I would love to hear comments from our participants. If you wish to raise your hands, please feel free to do so, and I will give you the floor. I see Hadia asking for the floor. And then Jan and Holly, in the order of our agenda, if you have any comments or thoughts you would like to add—and these do not have to be in a presentation format—do feel free to do so. Hadia, the floor is yours. Thank you.

HADIA ELMINIAMI:

I don't know much about the patent of Verisign. I haven't actually looked into it thoroughly. But my understanding, it basically addresses the issue of the thick registries. And Verisign moving into a thick registry, I think it was in its best interest to come up with such a patent. However, if I look at a system like the SSAD or maybe similar systems, I don't see them really in need of such a need to use the patent actually developed by Verisign.

Again, maybe I'm missing something. I don't know the exact details. But that's from a quick look at the paper that you put in the chat. So as a

thick registry, if they go ahead and use it, of course, it's their patent. But again, I don't see the benefit of that patent to a system—or not the benefit but necessity of such a patent for a system like we're thinking about. The benefits are clear, but the necessity to use it, I don't know. We have other options that are simpler and I would say cheaper, maybe.

JOANNA KULESZA:

Certainly. I think that the potential there is for Verisign to want to use it, not as much as us being encouraged to follow that lead. The question is whether the patent might impact the way we do policies here within ICANN. Jan, I'm curious if you have anything to add.

JAN JANNSEN:

It's a really good question, and it's a very difficult question as well, because a patent, typically the way it works is that you have certain claims that are protected by themselves. So if certain aspects of what they're claiming are protected and they invoke that protection in the way that that—some of the concerns by the community and the development of SSAD are being thought of and they say, "Yeah, but that aspect is something that is patent protected ..."

The future will tell, and the future will also tell whether that is something that can be invoked, will be invoked, will also be protectable and will stand scrutiny of a court if necessary. But I see your point, Hadia. The patent was not designed to replace SSAD or to ... So let's

hope that it will not, and so far, I think we don't see signs that Verisign is trying to use this to prevent an honest discussion about new policies.

But indeed—and I wanted to comment, if I may, Joanna, the fact that you're saying—and also, Christopher raised this question at the beginning, it is taking so long for the EPDP to resolve. I have some thoughts on that as well, and I think one of the reasons is that ICANN has not looked at GDPR until it was “doomsday.” And then it took a rather drastic decision by having the temporary specification in place, which was actually getting rid of everything that existed before in the WHOIS environment. And because that decision was so drastic and so friendly towards registrants who want to remain hidden, that really changed the ballgame.

It really has become extremely difficult to have some of the drastic decisions that were taken at kind of a rushed basis to get them reversed or watered down, and I think that is maybe the main reason why this is taking so long. The decision was there from one day to another, so drastic to avoid any kind of liability risks, and now to have that decision scrutinized, that is really something that this community has difficulties in doing.

JOANNA KULESZA:

Thank you, Jan. I believe there's a follow-up question from Ken-Ying, and I'll give the floor to Holly to try and wrap our heads around the policy implications, but I think this is a follow-up question, so I'm just going to pick it up here. “How would Verisign license the patent to ICANN members? Can each registry obtain it for free or at a low cost?” I

think there's a relatively simple answer. I'm curious if you want to pick it up, Jan.

JAN JANNSEN:

That is something they could do. They could also relinquish their patent rights. It is a legal title that they have, and they can basically do whatever they want to do with it. But anyone is also free to attack a patent, obviously.

JOANNA KULESZA:

Thank you very much, Jan. Holly, I'm curious if you have anything that we've missed and should be added for us to be able to better represent end users' views in the policy development process.

HOLLY RAICHE

I'm not sure. I'm just following the chat, and there is a discussion that interests me. Lori Schulman, who I'm reading talks about the Booking.com decision, there's some really good discussion about that. I don't know if she wants to talk about that, but there are some questions that follow that in terms of when I was talking about trademarks and the extent to which, circumstances in which a domain name might be seen as a trademark, to me, that's a very interesting question, and I'm just wondering if Lori wants to talk about it. Certainly, Jonathan does, and I'm happy to talk about it as well. It's just IP lawyers talking.

LORI SCHULMAN:

Yeah, I was just putting some responses in to comments in the chat, but happy to speak a very little bit about this. The whole idea of domains as trademarks, as it has a fairly long history and there's been evolution in thinking over the course of time, but that being said, in terms of domain names functioning as trademarks, yes, the law has evolved. Decisions that were taken today wouldn't necessarily be the same decisions that were taken 15 or 20 years ago, because the nature of commerce on the Internet has changed.

And one of the things that have changed is that consumers now look to domain names as trusted brands, that when we see something like Booking.com, enough of the consuming public knows that this isn't purely an address, this is a source for a service that people trust to—and I'll use the generic term—book their travel.

So the question then becomes—and there's different variations of trademarks. Sort of the basic trademark 101, you can have a trademark that's very distinctive that may not have a particular meaning and develops a meaning over time. The classic one that is used is either Xerox or Kodak. When someone adopts Xerox or Kodak as a name, it's made up, and it becomes famous because people have bought services or machines or whatever and over time, we know Xerox means something and Kodak means something.

Another great example of a good term is Google. Google has a dictionary meaning, but when used the way that the Google search engine uses the term, it becomes unique for search and other services that Google offers. And there's a line all the way down between what

they call very coined phrases and automatically distinctive phrases that may be more descriptive or tell you something about a product or a service, but over the course of time, that term becomes so associated with a product that the public then starts looking at that as a brand.

And a great example of that in our space is Microsoft Windows. Initially, windows was a technical term, but then the way Microsoft used it and the amount of investment they made in associating windows slowly with their offerings, window became a trademark. And I would say that's where we are today with Booking.com. You have a term that's normal and ordinary that everybody uses, booking, and then you have the gTLD extension, .com.

And the legal question was, well, when you put these two things together, Booking.com, does it mean more than an address? And the decision in the United States was yes, it means more than an address. And whether or not that's good or bad—there were comments in the chat that this was not a good day for trademark law. That's debatable. It's always debatable. That's what's great about the evolution of law, is that we can debate these questions.

But today, right now, the Supreme Court decision is a generic term like booking and a generic gTLD like .com, when you put them together and you invest—and you have to invest a lot, advertising, making sure there's quality behind your services, customer satisfaction, all of that is taken into consideration.

So if somebody were to register, I don't know, travel.com today, today is the first day they own it, they wouldn't automatically be distinctive.

They have to develop it, and that's what the law says. There's something like Google that can be almost immediate, and there's something like Booking.com that takes a lot of time. Same for Windows.

And I'll leave it there. I know we have very qualified IP lawyers on the panel today. But I'm also happy to field any questions.

HOLLY RAICHE

That's absolutely perfect. I don't know, Jonathan, if that answers your question. I'm not sure if I can give you a definite yes or no. It really depends on the circumstances, it depends on the acceptance of the name as a particular quality, it depends on the sort of things that any court would look at in trying to decide, is that accepted, does it mean something over time, and so forth. So the answer sometimes to things is I don't know, but it depends. And that's a [inaudible] answer, but lawyers do that.

JONATHAN ZUCK:

Thanks, Holly. Yeah, no, I was just trying to understand what would make that a good or a bad decision, because intuitively, it seems like it would be okay to allow a Booking.com to trademark that name in order to protect it from the misuse of the name in total. So I was trying to think what it is that could be the downside consequences of allowing that name, because we have a situation now, obviously, where Coca Cola has cocacola.com, but they can also use their trademark to say you can't register cocacola.contests or something like that, right?

HOLLY RAICHE

Yeah.

JONATHAN ZUCK:

So the question, I guess, I had that was my guess at what might be a downside consequence to that Supreme Court decision is, does this empower Booking.com somehow to suggest that booking.travel for example would be a violation of its trademark because it's confusingly similar, or something like that, which would then feel like a pretty serious downside to having allowed them to trademark what was primarily a generic term.

HOLLY RAICHE

Jan can answer it. I can too, but I can probably give you an answer arguing both sides. So, which side would you like? Seriously.

JONATHAN ZUCK:

Is that a serious question?

HOLLY RAICHE

Well, no, it's a serious answer because I can make arguments saying the fact that there's dot something else there and that's also used in a similar way over time may negate the way that the particular Booking.com matched a Supreme Court test. But I can also foresee a situation where over time, it may actually mean something different, is accepted to mean something different. And if you're looking towards those indices, you might be able to argue it.

It depends on the use, the acceptance and so forth, exactly the tests that Lori was talking about. So [inaudible]

JONATHAN ZUCK: Right. I don't think I'd be able to get a trademark right away for booking.travel. I mean, would I be somehow challenged in a UDRP proceeding for trying to even register that domain?

HOLLY RAICHE Probably up front, yeah. But as you know, I can argue either way.

LORI SCHULMAN: Holly, do you mind if I jump in real quick about that?

HOLLY RAICHE Oh, Lori, go for it.

LORI SCHULMAN: Sure. about that particular case, is that when that case was argued, Jonathan—it might interest those who are really interested in getting in the weeds of this to listen to that oral argument, because it was a very interesting oral argument, where Booking.com itself admitted that, were it to win, there would be an extremely narrow interpretation with very limited ability to enforce. And I don't know if they would feel it—and it's up to them, it's a business decision whether to go after somebody in a UDRP, but I can tell you that they would watch the site

to make sure it doesn't evolve into a lookalike or something where you could add more evidence to it.

But I would say on its face, probably not. I would actually go to an extreme here, I would commit a little more than Holly on that one.

JOANNA KULESZA:

Thank you. This is really interesting. I appreciate the fact how we managed to merge the topic and look at this issue from various angles. Now, again, I have been designated as the timekeeper. Thank you very much, Holly, for inciting this lively discussion. I see Christopher's hand is up, and clearly, I'm reserving time for Christopher to give us a summary. And there is another question that just popped up for Jan. I'm going to read it out for interpretation purposes, and then I'm happy to give the floor to Christopher to try and summarize this interesting and yet diverse discussion we've been having. I feel like there's also a jurisdictional context to this.

Jan, the question we have from Sayed, "In the WHOIS data, the registrant of a domain name information keeps confidential, and even the name, title of the firm. This is somehow the hacker exploits this privacy provision under GDPR in WHOIS data registration. However, it is very difficult for the users, especially a victim of fraud from a fake online shopping with a domain name whose most information is hidden under tag of privacy in WHOIS data and victim user is unable to see the important information from the WHOIS. The question is, how we keep balance in WHOIS data privacy as per GDPR so that registrant

of a domain name can enter the basic information which is visible to the Internet users?”

I think it's a very general question on WHOIS. I know Jan has been involved in the EPDP. I'm going to give the floor to Jan to try to give us a substantial yet brief legal response, and then I'm happy for Christopher to take the floor. Thank you, everyone.

JAN JANNSEN:

Thank you, Sayed, for that question. And really, I think this is one of the main challenges that we see today: how are we finding a balance again? Because probably, before the temporary specification, there was not enough balance and there was not enough attention to the privacy of personally identifiable information. I think that's correct.

However, the balance has shifted completely, or the scale has shifted completely in the other direction, and this is something that clearly, the EPDP has failed to resolve to date. All our hopes are in SSAD to correct these situations where also for law enforcement agencies so that at least they can have access to the full and accurate records of who is behind a domain name registration. And I think that this entire community still has a lot of work to do in ensuring that accurate data is being collected and that the data is being published to a certain extent, and also then disclosed to another extent to parties with a legitimate interest, because that is also what GDPR is calling for.

I think Hadia was explaining that we need a purpose to collect and publish or disclose data, but these purposes, they do exist, and there are

numerous legitimate reasons, as you have just stated, Sayed, to have this information available, and also available not only to law enforcement authorities, IP lawyers like me, but also to a certain extent that consumers are empowered and they can identify whether they are visiting a website that is legitimate or a website that is potentially fraud.

And for that purpose, I think that the current discussions about distinction between legal versus natural persons in EPDP phase 2A is quite important, because if at least you have the information from a legal person that is verifiable, that you can see, okay, this is a legal person that has registered that domain name, that is the person who is behind it, and these records, they are to a certain extent disclosed because they do not fall under the protection of GDPR, I think that's really the way we should go. But unfortunately, we see that others in this community see things differently.

JOANNA KULESZA:

Thank you, Jan. I would be eager to give the floor to Christopher to try and summarize this discussion. I know we are tight on time, and I have due regard for the timing of our interpreters. Christopher, if you would give us a brief summary, that would be wonderful.

CHRISTOPHER WILKINSON:

Well, first of all, thank you very much to all the panelists and participants who've contributed to this debate. Secondly, I'm quite sure that we've not heard the last of this one. I think the At-Large community and together with registries and registrars and other

operators, and dare I say, European data protection offices, they will want to follow up on some of these issues.

With such limited time and my very limited legal knowledge, I don't feel competent to actually summarize the main legal presentations and discussion that we've had. And I think it will be important, first of all, for Gisella to maintain the files of the presentations and that we should have access to the chat. I very rarely refer back to the chat, but I think on this occasion, it's quite important to check on some of the issues that have been raised [inaudible].

I would also draw attention to the scale of these issues. First of all, whatever the software interfaces are between registries, registrars and the personal data of registrants, there's a lot of it. And those interfaces are multiple. And I know from other implementations that registries and registrars really don't want to have a different software implementation for different top-level domain. Professionally, technically and economically, that becomes completely unmanageable, which is why I did introduce the idea of having an international standard and in this context, it should be an IETF RFC rather than a patent.

The other issue is basically the privatization of generic words in English. I have pretty strong reservations about this tendency. .com is the largest, but it's by no means the only top-level domain. The English language in the United States is an important part of the global culture. But it is by no means the only implementation of English and is certainly not the only implementation of language. And I think we need to build

into the domain name system and indeed into the software implementations a very clear recognition that it won't all be in English and it won't all be subject to national patents, whether it's in the US or in the European Union. Things will be more complex and difficult to regulate. And off the cuff, I don't know whether this is ICANN itself, the UDRP, or WIPO, or other fora, but I see problems down the road if we try and accept that putting a generic word with a .com top-level domain ipso facto creates the preconditions for a new trademark. No, that doesn't make sense in the long term worldwide.

I notice that we have 135 participants on this call. Thank you all for joining us. I think your diversity throughout this exercise emphasizes that this is not only an English language issue, it's not only an American intellectual property issue, and we all need to ensure that the user community in all countries and in all languages do have an understandable, easy, and as somebody pointed out, inexpensive access to the domain name system.

So, Joanna, thank you very much for taking on this complex and difficult task. I think you've made a great success of this session, for which I also thank you and our participants. And I would rely on the staff to make sure that in terms of transcripts, references and links, the backup will be there, because I think Joanna, and perhaps with the help of one or two of the participants, would like to have a report that can be, first of all, a definitive milestone in this debate, and secondly, accessible widely to the hundreds of people who are concerned by this issue but who are not on this particular call. Thank you, Joanna.

MICHELLE DESMYTER: Thank you so very much. Today's meeting has adjourned. Thank you.

[END OF TRANSCRIPTION]