KOBE – At-Large Leadership Policy Workshop 2: Balancing privacy with security and stability for the Internet end user
Sunday, March 10, 2019 – 10:30 to 12:00 JST
ICANN64 | Kobe, Japan

YESIM NAZLAR: Hello. Welcome to our second session. My name is Yesim Nazlar. Before we start, I would like to make a reminder, as usual. So, as you know, we have English, Spanish, and French interpretation for today's session. So, please, don't forget to state your names before speaking and also please don't forget to speak at a reasonable speed to help our interpreters. And if you would like to stand in the queue, you may use your tent cards like this. Place them at your tables, please. That's all I have for now. I would like to now leave the floor back to you, Jonathan.

JONATHAN ZUCK: Thanks, Yesim, and thanks everyone for coming back from the hallways conversations. I hope they were productive. With respect to the last session we had, Glenn McKnight has started a Google Doc for people to just share their thoughts and quickly jot down things. So, he's going to send that around to the group a link to that so that you can just have this kind of communal area to share your notes from the last session, so that anything you

didn't get to say or thoughts after you think about what was said. So, I will do that for both these sessions. Thanks, Glenn.

This session is, again, meant to be an internal At-Large discussion about where we are and what we're trying to accomplish in the context of the next steps for GDPR. We have some guests here that have expertise in these areas to help provide information to us, but we'll take this conversation beyond that and probably do more parsing of this after this morning but I wanted just to get this conversation going, so that we're all saying the same things to the extent possible going forward.

Also, this came up a little bit in the last session as well. Let's do our best not to relitigate phase one of the EPDP as well, but be constantly looking forward to the extent that we can.

So, the At-Large challenge, one of the many, as we've had discussions about that is that we seek to advance the interests of "end users". There are both registrant and non-registrant end users. So, there's a lot more non-registrant end users and these interests aren't necessarily always aligned and that could be up for some conversation but that's where we've been on this issue.

We also think that non-registrant end users have been underrepresented in the discussions, so if nothing else, we're trying to be the voice of those non-registrant end users so that

they have a voice in the discussion while not saying that the registrant end users are unimportant or anything like that.

So, we've determined to be the voice for that. So, for this exercise, if possible, what we're trying to do is really discuss the issue from the perspective of non-registrant end users and I think there's a lot of ways to approach that but that's what we're going to try to do, given that we've made the decision to back those folks. That's what we're going to try to do.

The issue of non-registrant end users is it's actually all of us, including registrants. So, when I'm registering a domain name, I'm a registrant. When I'm booking airline tickets, I'm a non-registrant end user. So, I think it's better for us to think of end userdom not as some collection of people that are unsophisticated but just a set of tasks that people – all of us – spend the majority of our time doing whether we're the founder of the Internet or my aunt Donna. We still spend a lot of our time engaged in end user activities, whether it's e-mail or online banking, online shopping, discussion groups, etc.

So, it's really about advancing the interests of those activities and facilitating those activities rather than saying this person is an end user and this person isn't. So, that's the perspective that we're trying to take as we move forward through this. Next slide.

So, in the path forward, phase one is complete. I know this is very high level and everyone will have corrections to what I'm saying, so just count to ten before you make those corrections because we're trying to think forward. But phase one is complete.

So, we have basically decided the valid reasons to collect data, which data will be public and which will be private, where GDPR applies, kind of. That's still something that's being openly discussed. And to whom GDPR applies. So, this is legal versus natural and where is this geographic thing that I know there's still some open debate about.

As we look forward into phase two, who will have access to the private data, the data that's been determined to be private, and under what circumstances will they have that access and using what mechanism? And those will be the discussions going forward. So, if anybody wants to make a real substantive change to that very broad stroke, I invite that now. Thanks. Next slide.

So, who would like access to the data? Well, law enforcement are interested in access to the data for consumer protection purposes, cybersecurity researchers for security and stability purposes, reputational systems that do block listing and things like that, that help protect our inbox from spam, malware, and phishing, and IP owners for their own interests, but also with consumer protection implications. We've had some discussions

about this yesterday and we should get that out front as well. We're not necessarily advocates for IP for its own sake but there is implications for malware, fraud, and counterfeiting that do interest us from the perspective of end users, so that's part of the discussion as well. Next slide.

So, the first little discussion I wanted to have was about law enforcement. So, some of the questions, just to get the conversation going, are how have law enforcement used registrant data to date? Are there other ways to get the data rather than registration records? Is law enforcement automatically covered under GDPR so we don't need to be talking about them so much? I've heard that argument as well. And how has the effective blackout of WHOIS affected law enforcement efforts over the past year. It's not a long sample, but we've got a little bit of a sample of how things have gone and I'm curious if anyone has any information, anecdotes, etc., on that issue.

So, what I may do is start with Maureen to get your perspective on some of these kinds of questions and then open it up for counter points on these questions. And it's just a discussion and we nobody needs to win. We're just trying to get more information out. So, yeah, I'm looking at you. To get some information on the table, so that when we are having these discussions going forward about how we're going to approach the next phase, we're

doing it with facts on hand and not just the rhetoric and the vitriol that has surrounded the process. So, Laureen, I'm going to give it to you fist.

LAUREEN KAPIN: Sure. This is Laureen Kapin and I appreciate the opportunity to be here and speak with you about these important questions. I am an attorney for the United States Federal Trade Commission which is the leading civil law enforcement agency in the US that deals with consumer protection and privacy. We have those dual mandates, at least from my side of the Federal Trade Commission. We also have a competition focus but I'm not involved in that.

So, I am not in it to win it today but I would like to share perspectives on why WHOIS is important to law enforcement and consumer protection authorities. I especially really appreciate the emphasis that the At-Large community has chosen to take on the non-registrant end users because it's kind of like the Dr. Seuss book, The Lorax, who will speak for the trees? Who will speak for the end users, which in a sense is all of us. And I do agree with the observation that Jonathan made, that end users are underrepresented in these discussions. The end users, of course, are really part of the key mandate for the Federal Trade Commission which really seeks to protect the public from

deceptive and unfair practices, i.e. we don't want people to get ripped off and we try and protect them when they do.

With that said, I want to move into how law enforcement relies on the WHOIS and then we can move into some of these other questions and these are things that I know you've heard before, so I'm not going to go into nitty-gritty boring details.

Basically, our agency uses WHOIS as an investigative tool and we use it as an investigative tool for everything from mortgage refinance scams – i.e., folks who are trying to take advantage of people with low credit or no credit by offering them opportunities to get a lower interest rate when in fact they're just trying to rip them off. Very often these sorts of scams are perpetuated through websites or e-mails and the WHOIS had been one of the first places that the FTC had looked when they want us to answer the question: who's behind this domain website that's trying to rip people off?

Significantly, we also rely on the WHOIS when we are investigating privacy violations. For example, spyware matters. If an entity is trying to install spyware on a user's website, again, we would loo to the WHOIS for attribution. Who's behind this phishing attack that led to the installation of spyware that infringed someone's privacy? So, we use this in all of our jurisdictional mandate to protect the public and I want to

emphasize that that's not just for frauds and deceptive cs. It's also for privacy violations.

But we're not the only law enforcement agency, of course, in the US and around the world that uses WHOIS. I also polled my colleagues who are active in the Public Safety Working Group. That's my other hat that I wear here at ICANN. I'm co-chair of the Public Safety Working Group within the Governmental Advisory Committee.

And I heard from our friends from the US Secret Service has actually a fairly broad mandate, besides protecting the president and being the subject of a lot of exciting movies and novels. They also secure events that you and I may attend, like inaugurations, public events where political figures may be speaking. So, if there are threats that they detect at those events that have a connection to a website, they are going to use the WHOIS for leads in that investigation.

They use the WHOIS to identify patterns of activity. So, if there's a domain that they're interested in, they may try to use third-party tools to see, well, who owns that domain? Oh. It's Joe XYZ. What other domains does Joe XYZ own? And that becomes a key component of their investigation.

So, when there are threats to events or people, they also have a counterfeit … They investigate counterfeiting activities. They will use this as an investigative tool.

And I can go into all the different ranges of subject matter from business e-mail compromise to romance scams, which by the way are one of the biggest topics of people losing big sums of money these days. That's one of the top frauds going on in the world today where people fork over huge sums of money – romance scams. That's also e-mail based. Network intrusion cases. A whole variety of topics that the US Secret Service Investigates.

Also, the Department of Homeland Security which focuses on cybersecurity and a large part of its mandate, including the [certs] – those are the entities that try and protect the security of the domain system, particularly in the area of network intrusions. They use the WHOIS to detect and track domains associated with threats.

All this to say is that there's a broad range of activity that law enforcement and consumer protection authorities use to protect you and I from bad things happening. It's a really important tool.

Let me move on to two of these other questions, briefly. Jonathan unwisely has not given me time restraints and I don't want to gobble up—

JONATHAN ZUCK: I will eventually.

LAUREEN KAPIN: Yeah. I don't want to gobble up the time unduly. Are there other ways to get the data other than registration records? Yes. There are other ways we can seek subpoenas or use our civil investigative demand authority that is sort of like a civil subpoena and those are important tools but they're very time-consuming. They involve going to a court for some sort of approval and it is something that takes much longer and is more resource intensive than looking up a name in a database that used to be done in a matter of seconds. So, there are alternatives, but they take much longer and they involve a lot more resources which means that less investigative work is going to be done in the same amount of time, and when there are critical emergencies, it's not feasible to be in a position necessarily to wait the weeks that it may take to actually get your subpoena approved, issued, and responded to.

I'm going to skip over the last question because I think Greg is probably going to give a lot of information on that, but I do want

to address the third question because it's really important and it's a big issue. Isn't law enforcement automatically covered on the GDPR so they don't need to worry their pretty little heads about it? No, that is not the case, especially for foreign law enforcement.

So, the GDPR absolutely recognizes the balance that needs to be met in protecting user's privacy and the need for other entities to get access for that information but it's very worrisome that the term public authority under the GDPR has not been interpreted, so far as I understand it, to include law enforcement authorities that don't come from the EU.

So, if you're from the EU, there's absolutely a path that is written into the GDPR for you to have a justification for getting this information. But it's very unclear if foreign law enforcement have that same path.

Now, the GDPR is very long, very complicated and still is going to be interpreted by judicial entities in the EU, so things are somewhat at flex. But my understanding is that there is no clear path for foreign law enforcement to be able to obtain information under the GDPR and that's a big problem, particularly for someone from the US, a civil law enforcement like I am.

So, that's a preview about how law enforcement uses WHOIS, how it's important, why other methods are less efficient and

actually won't let us do the work we need in the time we need to do and some of the really critical blank areas or obstacles in the GDPR for law enforcement around the world to be able to get the information they need to protect you and I.

JONATHAN ZUCK: Thanks, Laureen. I'd like to give it over to Kathy and [Farzi]. I'll let you work out between yourselves who best to deal with which topics. I know, Kathy, I've heard you say that the number of people that are bad actors is so small that WHOIS has historically been like overkill for [inaudible] that small group of people. And you've also mentioned the stakes being higher in some ways, that the rights in some ways might outweigh interests for lack of a better term, and that some of the downside consequences of revealed data might outweigh some of these interests we're talking about.

I'm interested in your take on our take but also how you're feeling about the law enforcement issue in particular, because we're going to take these one at a time. So, that's for both of you in whatever order. Thanks.

KATHY KLEIMAN: Great. Thank you, Jonathan. Just to let [Farzi] know, I'm going to give some background and maybe you can address some of the

questions here and we can address them together. Just a head's up.

I'm Kathy Kleiman. I'm cofounder of the Non-Commercial Users Constituency, so I've been coming to these meetings for way too long.

Let's talk about just a little bit of background for a second. If the Internet was just a stream of e-commerce, if all we were doing was buying and selling goods, that would be one thing. But the Internet is the greatest stream of communication known to mankind. I'm not the one who said that. The United States Supreme Court said that.

Years ago, in the United States, when we were still a colony of Great Britain, there was a rule that in order to have a printing press, you had to give your name and address and get a license from the British government. The reason they did that is if you said anything that criticized them, if you printed anything that criticized them, they'd come and destroy your printing press. We opposed that overturned that and created the Frist Amendment when we got freedom from England. The reason we did that was not to protect the printing presses. We did it to protect the end users. We did it to protect the people getting the communication, so that they could get free and open communication from various newspapers that wanted to tell them what was really going on

because newspapers in so many countries oversee the government. They're the people, they're the citizens, questioning, investigating what our governments are doing.

Years ago, I represented a human rights group that was publishing information about corruption in their home country. They were out of the country but their families weren't. Their domain name was talking about the sale of public resources like mines to private people who are in the President's family. There was a lot of corruption. There was an upcoming election that was going to be monitored by international election monitors.

So, they were trying to get information into their country via their domain name. Their website was listed as one of the top ten treasonist sites in the country but it was the only place you could get good information because the media was controlled by the president.

They came to me. They said that if it was known who was behind that website, their families would be arrested the next day and we did everything we could. We were very concerned about the public WHOIS and this was the days before proxy and privacy services.

I am very concerned about what is in the WHOIS database and when I was director of policy for dot-org, I got up in front of

international law enforcement and I said, “We have a problem. I can work with my law enforcement in the United States,” which is where dot-org was based, “Pursuant to due process. I know what the rules are.” But when China comes to me or when any law enforcement comes to me and says, “I want information,” or, “I want take-downs because it’s a violation of my criminal law,” I can look at them and say, “Wait a second. It’s a violation of criminal law in China to have pro-democracy websites. Am I supposed to be taking them down?”

So, I pose to you the problem of global law enforcement. There is no global law on this. And not all law enforcement operates the same way. We have due process for a reason. We don’t give law enforcement in the United States or in any country I know unlimited access to anything. There’s a process because we have our protections and those protections protect us as speakers but they protect you as end users receiving our speech.

I can say much more and would be happy to if there are questions. GDPR does offer us a balance and does provide much more protection, and yes it’s really hard. The WHOIS database was created before ICANN. It was created before any of us. It was created when the National Science Foundation ran the network and it was a trusted network. It was all trusted people and none of it was personal data. I’ve talked to them. It was the IT

department at MIT and the business address and the business phone number. There was a lot more here.

I just pose to you the question: would law enforcement ever kill journalists? Thanks.

JONATHAN ZUCK: Thanks, Kathy. I guess, just for further context, again looking forward, we don't any longer have a public WHOIS, so it's more like are there solutions for gaining access to data that will be better now going forward? Because the idea of it just being public, we have set aside at this point. So, I just want to keep the conversation in this forward-looking thing as opposed to indicting the thing that's already dead.

KATHY KLEIMAN: Well, but what I'm hearing a lot – and I'm sorry, it was in my head but I didn't make it expressed – is law enforcement wants unlimited access to the WHOIS database because they're law enforcement. Law enforcement in the United States is telling me this as well as law enforcement overseas. So, they want that WHOIS as if it were public. I'm not passionate on this subject or anything.

They want the WHOIS as if it were public. They want that unlimited, all-you-can-eat access to the WHOIS. And that's kind of a starting point that I'm hearing. I think I still heard it from Laureen.

LAUREEN KAPIN: I didn't say that at all, Kathy.

KATHY KLEIMAN: Okay, but I've certainly heard it from a lot of law enforcement. So, how do you get the balance? Even of law enforcement, where are we, how do we ask? And as ICANN, how do we ask the right questions of law enforcement and what is due process when you're talking about a private multi-stakeholder organization asking questions of some of the most powerful government organizations in the world.

JONATHAN ZUCK: Is there anything you wanted to add? Introduce yourself, too.

FARZANEH BADII: Farzaneh Badii, Non-Commercial Stakeholder Group. I just want to make it clear that the important mission of law enforcement is acknowledge we are not discrediting their work. However, of

course not all law enforcement agencies around the world are accountable and we know that. So, there should be measures in place to hold them accountable if they abuse access to the data.

That is very important for us. However, what we do also keep hearing is that WHOIS is being used for purposes that are not really in ICANN mission. Now, that is a very controversial thing and I know we are conflicting on this issue, but this is my idea.

The other thing that I wanted to say is why do we always think that privacy and security are at odds? [Why do we need] a balance? They are not at odds.

So, if you want to do security work, then we should have measures in place to disclose the data to the legitimate interest holders and not to have data out in public and just publish it. What I found concerning I think for the past 20 years, there has been a push. There was a push for WHOIS to always be public. So, there was no balance to be sought and the actors that wanted WHOIS data to be public – and this is personal information of domain name registrants. It's their name. It's their number. It's their phone number. It's their e-mail address.

Also, when you look at … So, I think that the other actors, it would be good if they could also acknowledge that maybe privacy of domain name registrants also is important for the end users.

And one point I just wanted to make, last one. When we talk about, for example, domain name hijacking rate has gone down after WHOIS has gone private and there's data on that, you might want to dispute it. So, it's not that black. It's not that black and white. And there has to be a balance between when we are talking about the bad things because of WHOIS being private and the good things that happen. That's it. I had another point I wanted to make, but do I have time?

JONATHAN ZUCK: Related to law enforcement or?

FARZANEH BADII: Yeah.

JONATHAN ZUCK: Okay.

FARZANEH BADII: So, also, for the law enforcement access to data, you mentioned, John, that WHOIS data is redacted everywhere and we don't have to go back and re-discuss the issues. There are attempts at the EPDP to kind of do geographical differentiation and just say that GDPR doesn't apply in these regions, so it should not … So, those

domain name registrants, their data should be public. So, no, we have not really solved the problem. That's it.

JONATHAN ZUCK: Okay. Thanks, Farzi. Did you want to … It sounded like you were trying to hand to Greg for part of this. I was going to wait and do the research questions, Greg, but did you have something you wanted to add to this conversation going forward?

[GREG]: I can wait.

JONATHAN ZUCK: Okay. Does anybody have questions? You've sort of heard both sides of this in the law enforcement context. We're going to move on to the other context, so don't ask questions about those yet, but do you have questions for these folks on these points related to law enforcement access? Olivier?

OLIVIER CREPIN-LEBLOND: Thank you very much, Jonathan. I'm going to ask a question to Kathy and you're going to hate me for this and I'm really sorry already in advance.

In 2016, Kaspersky Labs have recorded 758 million instances of cyber attacks. How many people have been jailed directly related to WHOIS records being made public in that year or in recent years? Because I can't imagine it's that many people.

FARZANEH BADII: I have a question. What do you mean by cyber attack? Because not all cyber attacks are handled by WHOIS. So, we have to be a little bit more nuanced. And you want us to give you data on how many people have been jailed, minority groups that have been jailed in autocratic countries because of [access to data]. Yeah, sure.

There is also harassment issues. So, I cannot give you, because this data doesn't get published – a government doesn't come and say, "Oh, so [inaudible] WHOIS personal information of domain name registrants and I jailed this many." So, I'm sorry, no. But there are examples and we are documenting them. And we don't want to say there is cyber doomsday when WHOIS data is just available publicly, but there is a risk.

OLIVIER CREPIN-LEBLOND: If I may add, it's a good answer. At the end of the day, I generally wish to know how much there is. I mean, it would be a good thing for civil society to try and track these things and see.

FARZANEH BADII: Even if one person gets jailed because of WHOIS and domain name registration, we have to be concerned.

OLIVIER CREPIN-LEBLOND: So, maybe we should do the same thing or look at it in the same way with regards to cyber attacks and spam and malware and this sort of thing.

JONATHAN ZUCK: That's right. I think we have conversations going forward about the stakes that are involved as well. So, we need to make sure, because obviously the stakes in this case are higher in many instances than they are in that case and trying to have that conversation is worth doing.

UNIDENTIFIED MALE: [off mic].

JONATHAN ZUCK: Okay. Dmitry, then, first. Andrei?

ANDREI KOLESNIKOV: I am not Dmitry. I am Andrei. Okay. I thought it was a joke. Very short notes. I'd like to ask everybody to bind to the subject of today's conversation and meeting. We're not talking about jailing, imprisoning, or violation of the minorities or majorities or whatever. We have a subject and I'd like everybody to [inaudible] the subject. Thank you.

KATHY KLEIMAN: Law enforcement is always a question of law enforcement rights vis-à-vis citizen rights, so I don't understand why we're not on topic. If you only want to talk about law enforcement, we can leave, but we're here to talk about the balance that's been struck throughout the history of civilized countries.

ANDREI KOLESNIKOV: Alright. Sorry. Maybe I was not clear. We do have some factual data on the changes [inaudible] the GDPR involvement and temporary specification, etc., and this is closely related to ICANN activities and I'd like maybe to focus on this one because this is more important. We have a short time. We have Greg here. We have some data in hands. Why don't we just focus on the data and things and facts?

KATHY KLEIMAN: We haven't been given that data.

JONATHAN ZUCK: Thanks. Let's not try to confine things too quickly. We are a very broad community, at large, and we are not entirely on the same page about these issues. So, part of this exercise is to get facts out in front of people so that we can have further discussions and reach consensus going forward. So, let's try to do that. But, who do you have? Ricardo, okay.

RICARDO HOLMQUIST: I'll speak in Spanish. Sorry for that.

UNIDENTIFIED MALE: [off mic].

ALAN GREENBERG: Can we keep on the topic, please?

JONATHAN ZUCK: Yeah. Let's roll. We've got to keep going.

RICARDO HOLMQUIST: Sorry. My question is the following. For the first speaker, I apologize, but I cannot see your name. I think it's Laura. Laureen,

sorry. So, my question is are there any statistics on the data you refer to? Because as it happens with human rights, we have a serious problem when countries and especially not fully democratic countries, can have [inaudible] WHOIS data versus countries like yours which may be more democratic. But how many times do you have to access WHOIS to do something? Once a day, once a month, 100 times a day? Are there any statistics on how that is being used and what is the impact this has? Because if it's once a day, if you to a judge for the [inaudible], it doesn't seem to be a serious problem, particularly in countries like mine where you can go to jail just because you didn't go to court. You opened the WHOIS directly without a court order and the person goes to jail. We have to strike a balance. That is why I wanted to know if there are any statistics on that. Thank you.

LAUREEN KAPIN: Thank you for your question. I am sure that there are statistics. I couldn't give it to you at the ready, but what I would tell you from my discussions with my law enforcement colleagues, there are many agencies in the US and around the world who use WHOIS at least hundreds of times a day, perhaps more, because they have a large volume of investigations and that is the volume of the work that they are engaged in. Other agencies – for example, mine – may use it less often but there is a very large range in how

this is used. I would observe that I doubt there are many law enforcement agencies that would just use it once a day, if they really have an active caseload on their plate. These are generalizations but certain agencies do keep statistics but I couldn't report them to you right now.

But I'm glad you asked that question because I also wanted to acknowledge the very valid points made by my friends on the other side of the table, Kathy and Farzi, that these are very important issues and in terms of misuse of WHOIS, in terms of how people can be put in parallel – and I love your example from the starting days of our country because that's such a dramatic example about clamping down on decent.

That said, I don't think that there's anyone – I can say this I think with confidence. I don't think there's anyone in this room who would support the use of WHOIS to clamp down on free speech. That said, you're acknowledging that it's a risk and I think it is a risk that we need to deal with. So, I wanted to make sure that in my statements focusing on these harms – financial harms, physical harms, all these instances that are documented by the statistics about network intrusions, malware, phishing, farming, all those bad things to rip people off and harm people and that's separate and apart from child exploitation and other even more serious infringements, that there's a balance and the work that

the community is doing is to try and strike the right balance. I'm talking from a law enforcement perspective where I'm in the US and we are focused on trying to protect the public, but I do want to acknowledge the very fair points made by my colleagues that not every government has the same priorities and it's a reality we have to grapple with.

JONATHAN ZUCK: Thanks, Laureen. There's quite a queue that's starting to accumulate here, so I want to set some parameters if I can.

Since we have these panelists, let's treat this session like a fact-finding session and try to get as much information out of the panelists as we can and not use it as an opportunity to voice opinions, etc., because we will have other discussions about this with this information as resource. So, this is one that I thought was going to be the easiest and we had quite a bit of conversation about it.

So, I would hope that most of these questions are about gaining clarity from the positions you've heard from the panelists and not try to begin to debate the issue because we're going to have that debate, but let's try to make your questions about clarify, if you have it. Humberto?

HUMBERTO CARRASCO: Thank you very much. I'm going to speak in Spanish. I would wait because my question is for Farzaneh and/or Kathy. I will let [inaudible].

I think it was Farzaneh that said that at some point in time there were discussions about the use of GDPR according to regions. That presumably was according to the norms and there are other region where it is not applicable.

There is a conflict of extraterritoriality of the law. I am from Chile. Many Chilean lawyers said, well, GDPR is not applicable to us, but there is a case of other people, like Ricardo Holmquist, who has dual nationality. He is a Venezuelan and Italian national. So, this person is covered by GDPR even though he lives in Venezuela.

So, what is the issue here? The issue is that we will have to abide by the GDPR if we deal with Ricardo's data because he is a dual national. But how are you going? Is it you who handles the data? How are you going to distinguish who has dual nationality? That is the problem and that is why I have this question. What is the solution in such a case?

JONATHAN ZUCK: I'm not positive if anyone will have an answer to that question.

FARZANEH BADII: Jonathan, we do actually have an answer.

JONATHAN ZUCK: Okay.

FARZANEH BADII: GDPR does not actually – is not concerned with nationality, so it doesn't matter if actually Ricardo has dual nationality. GDPR is only concerned with the physical existence of the data subject within the European economic area. So, if you are a non-European citizen and you reside in the European economic area, then GDPR applies. But for European citizens not residing in the GDPR, not residing in the European economic area, GDPR does not apply, so it's not concerned with citizenship. And if it was, actually, it would have been very difficult. You actually need to collect the passport IDs of the data subjects. That's like impossible. Thank you.

JONATHAN ZUCK: Marita?

MARITA MOLL: Thank you. My question is for Laureen. You suggested or you're speaking about the fact that one of the barriers to letting go of the

WHOIS is going to take you a lot longer or somewhat longer to get the information that you need in the case of some kinds of violations and yet I'm thinking that in most democratic societies, this is a tradeoff that we commonly make. We ask for warrants if we want to tap telephones, warrants if we want to go into houses.

I wonder … It's very philosophical, but just because it's the Internet and everything goes so fast, now we have to have it instantly. We haven't got time anymore to take the time to do that kind of background work which has always been considered part of the tradeoff between privacy and security.

Is there really a lot of evidence that this would be a negative feature?

LAUREEN KAPIN: A couple of brief responses. First of all, we're not advocating going back to a public WHOIS. We acknowledged that the GDPR is a reality. So, part of the premise of your question seems to imply that I'm saying we should go back to the way things were and that's not accurate and I'm not advocating for that. So, that's one.

Yes, there is evidence that investigations are being hobbled, that they are taking longer, that there are real harms and I know Greg is going to speak more to that.

And for your philosophical question – and I love philosophical questions – we also live in a world where you and I, as people who are going to be giving sensitive information to folks over the internet, have a right to know who we're dealing with. And this is separate and apart from law enforcement. We also have things like phone books. We have business directories. There are lots of situations where the information we're talking about, not tapping phones which is a content issue but just contact – not content, but contact information – is something that we rely upon and expect and I don't think it's an unreasonable position to take at all that the public should have access to this information so they can deal securely and know who they're doing business with and certainly law enforcement which has even higher responsibilities than deciding what credit card they're going to use to buy those great new songs they want to purchase. So, I tried to cover the basis of your questions.

JONATHAN ZUCK: Thanks. We've got Alan next.

ALAN GREENBERG: Thank you very much. Two points. Hadia addressed part of Humberto's talk. The answer is more complex. There are those in Chile to whom GDPR may well apply. Not for their citizens,

necessarily, but companies. So, it's a complex issue. It's not simple.

In terms of statistics, however, the RDS WHOIS Review Team which should be publishing its report within the next 24 hours I hope. But they did a survey of law enforcement around the world and what's in the final report is not very different from the draft report which is public. That does have a fair number of statistics on how often WHOIS is used, what the impact is of not having it because we were doing it – did the survey just a few months after the temporary spec came in. So, we have some experience on both sides. So, there are hard numbers. It's a very preliminary survey. We didn't have a lot of funds, but it is a start at getting hard numbers.

JONATHAN ZUCK: Thanks, Alan. Holly?

HOLLY RAICHE: I would be interested in hearing from both sides. Now, I think most of us accept that in the United States and other Western countries that there are checks and balances. In fact, there is a recognized balance between the person [inaudible] information and law enforcement. I'm not necessarily saying it's met all the

time. It's probably fraying at the edges if not the middle. Forget that.

What kind of test would you put into the temporary spec to say we're going to allow those law enforcement agencies that actually respect an individual's privacy to have access and to say to the people who do not respect and who are likely to jail people, that in fact they're not going to get access?

That's the hard question but you're begging now for everybody to have access and I don't think we agree with that. I think we'd like a firm test from you and maybe from Kathy as well. How do you protect the people that the law, their own country, does not protect?

LAUREEN KAPIN: My colleagues seem to want to jump into this one first, so I will. It's a very hard question. I acknowledge that it's a very tough question. I don't have an easy answer for it. I don't know that there are easy answers for it. I wish I did. I do know that the work of phase two is certainly going to focus on, as Jonathan said, who needs access, why do they need it and under what procedures should they get it and I think those are the ways we're going to have to grapple with it. But it's a very, very tough issue.

KATHY KLEIMAN: So, I was asking Farzi what discussions have taken place on the EPDP on this issue because that's what I don't know. I would think some kind of tie to jurisdiction would be appropriate. Even if I'm not going to be happy with the outcome all the time. And I should say I'm an attorney. I'm a first amendment attorney in the United States.

So, at least … So, the idea that a registry and a registrar and a registrant can exist in certain countries with certain free expression rights and that the data of the registrant could be requested by law enforcement in an entirely different region of the world, maybe they're an expatriate of that country or that region. That just on its face is concerning. So, at least some kind of tie of the law enforcement to the jurisdiction of the registry/registrar/registrant.

LAUREEN KAPIN: The concern I have with that approach is that in terms of the scams and frauds and exploitation going on in the world, regrettably it doesn't just live in one jurisdiction. Law enforcement investigations are quite often these days taking place in multiple jurisdictions. So, a test that would be jurisdictionally based, i.e. law enforcement from the US can only get at information, folks in their jurisdiction. And if I've misunderstood what you're saying, correct me, but that's what I

understood or law enforcement in China can only get information on Chinese registrants. That doesn't to me take into reality the fraud and harms that law enforcement is investigating which are often international in scope. I would say that that would be problematic.

KATHY KLEIMAN: So, the response would be that I was an international law enforcement meeting I don't know about a decade ago and I raised this issue as well, that ICANN as an organization has to recognize [it operates] on a global level, but that law enforcement operates within the balances of its own countries laws and that the laws that balance and limit law enforcement in one country may not exist in other countries. We've already said that here.

But that means, while you may have scams and frauds coming in from certain countries, you're also going to have [dissonance] and people speaking and people who have escaped their countries. We also have genocide and we also have people who go after … We have countries dedicated to elimination of other countries and religious groups. So, the idea that one country can find out where all those religious institutions are, where they're located.

And by the way, GDPR doesn't just protect personal data. It protects sensitive data and sensitive data includes data about religion, about gender, about sexual identity, about political issues and morality issues.

So, a number of non-commercial organizations would fall under the sensitive protections of GDPR and you bet that law enforcement in lots of countries want to know where those organizations are. Thanks.

JONATHAN ZUCK: Hadia?

HADIA ELMINIAWI: So, I had a question. I think we haven't answered the how has the effective blackout of WHOIS affected law enforcement. Maybe we need to comment on that. I had a couple of points. So, actually, vulnerable communities, it's very important to protect them. There already exist many mechanisms through which you can protect vulnerable communities. Well, things like privacy-proxy and maybe not initially under this title but there are means by which vulnerable communities could be protected.

On the other hand, we should take a look at other citizen rights like human trafficking, child exploitation. So, it's not only the technical issues.

One last point. We all agree that WHOIS is dead and it's not coming back again and what we are talking about here now, law enforcement [inaudible] through a model or a mechanism to non-public data, and obviously through such a mechanism though we have not yet discussed anything in that regard, but obviously through that kind of mechanism, you'll be able to know who is accessing the data. So, which law enforcement is having the access to the data?

In case there is a violation to any kind of violation to citizen's rights, you should be able to actually hold accountable whoever is responsible for that.

Again, we are talking about a totally different system in which vulnerable communities will be able to be protected. As I mentioned, there's already mechanisms to do that, exist.

And with regards to the jurisdiction, tying of law enforcement to the jurisdiction, I have to first say that I have a technical background. I'm an electronic communications engineer, so I don't have any law background. But in some cases I think you

actually don't know the jurisdiction of the website prior to having some information about it.

So, this assumption that you do know the jurisdiction prior to taking the first step I think is not realistic. Thank you.

JONATHAN ZUCK: Thanks, Hadia. We're going to close the queue after the next question. Again, I want to reiterate that we want to really avail ourselves of the panelists and we're not trying to change their minds about anything. We're not trying to … We're trying to inform ourselves, so that when we have conversations going forward, they're as informed as possible. So try to keep that distinction in mind if we can. I don't want to make it a debate. I think I need to move on. Okay.

KATHY KLEIMAN: I should be deferring, Hadia. You're on the EPDP. You're following this very closely. I was co-chair of the first WHOIS Review Team so I'm following the old issues closely and that's what I'm bringing. Farzi is on the EPDP, so I defer to you.

But transparency alone isn't enough. That's an after-the-fact mechanism. The families are already arrested by then.

In the United States, we had a problem with chatrooms years ago because people were coming in, people used identities, identity names in chatrooms and other people were coming to the Internet service provider and saying, "I want to know who's behind that identity. They said something fraudulent about me," or, "They insulted me," or, "they insulted my company." And the Internet service providers were giving up those identities with no other process and the chatroom people went to court and they said, "No, you're not allowed to give up my identity without giving me a right to defend myself, and without giving me the right to go to the court as a John Doe or a Jane Doe which is a protected status, so that I can argue my rights and why I have a right to non-disclosure." Because after the disclosure, transparency isn't enough. I can know who it got to, but by then, my identity has been revealed and my safety and my security is now compromised.

By the way, they won those rights in the United States courts. Internet service providers never reveal an identity without giving the Internet user the opportunity to respond to the court.

So, I think we have to come up with something better and maybe my idea wasn't enough but we really need to think through these mechanisms and the dangers. Thanks.

UNIDENTIFIED MALE: Abdul, go ahead.

ABDULARIM OLOYEDE: Thank you very much. I come from the part of the world whereby you have lots of human rights [inaudible] governments, operations, and things like that. And I understand the fact that the Internet is the voice of the ordinary one. Well, when it comes to [inaudible], I think it's a different ballgame because I think human rights activists are probably those who classify themselves as civil societies are people from time to time, we know there is a risk with everything we do. With every action you take, there is a risk associated with it and human rights activists I think are probably activists in general are known to be people who are bold, to come out, express themselves, and that is one thing we appreciate about them.

I [inaudible] under the anonymity of the Internet, I think it's kind of something that is different. My question to this around the table is do you actually think advocacy should be done with anonymity? Because I think no should be the answer.

JONATHAN ZUCK: We're not going to, unfortunately, entertain that question. I think that's a huge philosophical question that we're going to have to discuss as a group because that's a big question. I want to move

on. I really thought law enforcement was going to be the easy one, so I was wrong about that. But thanks, everyone, for your active participation in this discussion. We have a lot to take away.

The next category, next slide. We've forgotten where the slides are at this point, probably.

So, the next category is the cybersecurity resource, research, and then maybe in conjunction with that, our reputational systems as well. So, I have them divided into two different categories but they might be part and parcel of the same thing. So, rather than wait for the slide, Greg, why don't you share some of the information you've gotten and some of the data in that context to get this part of the conversation started.

GREG AARON: Sure. Hi, my name is Greg Aaron. I'm a member of the ICANN SSAC and I was one SSAC's alternates on the EPDP. In my day job, I'm a cybersecurity professional. I work for a company that does the detection and mitigation of problems on the Internet and I've done a lot of mitigation in the DNS space specifically. I'm also a research fellow at the Anti-Phishing Working Group.

So, let's talk about some stats and about how people are being affected in this new world we have. One of the things I want to say is that a lot of the heavy lifting that's done to protect users on the

Internet is done by industry. I'll define research broadly to mean people who are trying to figure out what's going on on the Internet are trying to find the problems, the abuses, the cybercrimes, and that are dealing with those problems in various ways. So, using data of various kinds to find the problems.

Law enforcement actually gets involved in very, very few of the cases of abuse and cybercrime that happen each day on the Internet. They're focused on finding some perpetrators. But most of the problems are dealt with by the people who control the resources on the Internet. The Internet is a network of networks and those networks are companies, universities, governments, other entities who are actually running the services and they're the ones who actually deal with the cybercrime for the most part. A lot of that involves figuring out what needs to be blocked. You don't want certain kinds of things coming into your network and you don't want your users to go out and visit certain kinds of things, like scams and phishing sites.

So, finding those problems and then either blocking them or getting them shut down is what a large part of what security researchers are doing every day.

In the domain name world, the shutting down part is really important because what we're trying to do is find the domain

names that have been registered by criminals and getting those suspended so they cannot be used or cannot continue to be used.

Now, does anybody have any idea of how many domain names are registered by criminals each year? Any guesses? Millions. The answer is millions. I'll put a floor at at least five million. That's the number that are listed each year by some of the major blacklist providers. Those are the providers like SURBL and Spamhaus. Every one of us is being protected by those lists in various ways. They're keeping us from going to phishing sites in our browsers. They're keeping a lot of the phishing and malware e-mails out of our inboxes, that kind of thing. And that is a floor. The actual number is probably much larger because those researchers and services only find a certain percentage of the domain names that are registered by criminals.

Now, one of the main ways we figure out, one of the main indicators we have, has been the WHOIS information. Now, criminals usually fake their data. They don't put in their real names. But they're actually pretty bad about how they fake it. You can certainly find and identify a lot of suspicious domains by looking up that information and verifying or validating it. It's an indicator of bad faith, let's say, when somebody is putting false information, contact information, in the WHOIS.

So, that is a huge indicator. You can try to find bad domains other ways, by looking at what name servers they're on, but criminals will usually switch the name servers right before they start to do their activity and a few other ways. But it's been a really, really useful tool for a lot of years. And it not only helps you figure out what domains that might need to be looked at but also, in some cases, attribution to figure out who is actually behind the activity.

If I can, I want to show a couple of slides. What this is, is this shows what happened before and after the temp spec went into effect. This is data from Spamhaus which runs a block list for domain names. What the graph shows is the number of domain names that they were able to identify and then list on their service before and after the temp spec – before is in blue and after is in red. In this case, what their research indicates is they've lost the ability to find bad domain names and it's down by something like 60-70%.

What that means is they're finding fewer domain names and that means there are people out there being affected by those domain names because they're not getting blocked anymore. If you can move on to the next one.

Now, this is from SURBL and this is looking at listings in two domain names, two top-level domains – US and GDN – where the registries are not redacting the contact data. In other words, you

can still see it. So here, SURBL was able to continue to find and list domain names that were being used to do spamming and phishing and malware. So, this shows some success when you still have the data.

Finally, the last slide is going to show SURBL's overall success. You can go to the last one. So, SURBL had basically the same pattern as Spamhaus dis but actually worse. Before, the temp spec is blue. Red is after. And again after the temp spec, they lost the ability to find a lot of domain names, and overall the number domain names that are being listed on black lists is down which is going to translate into more harm to users. So, now that we've had some perspective since last May, we start to see the effects.

Again, when you're dealing with these kinds of problems on the Internet, speed is of the essence. We want to find these domains as fast as we can because we want to get them blocked or shut down. If we can't find them fast, that means that criminals are largely able to do what they want. And that is a problem.

Also, another thing to realize is that criminals tend to register more than one domain name at a time. I've seen cases and research done where a criminal entity registered 100,000 domains at a time. Now, if you can find all of those and you establish what they're doing, it is absolutely a good thing to suspend all of those. You increase the cost to them and you

deprive them of the resources that they are using to hurt people. And WHOIS is actually the best way to be able to do a lot of that kind of work. But reacting afterwards is a problem. So, speed and finding batches of domain names are two of the most important thing we need. And I'm done with those slides, thanks.

So, how do we have the tools we need but also comply with the law? That's the big question and that's a question that is going to be explored in phase two of the EPDP.

Now, the GDPR defaults to saying the data needs to be protected. The data subject has the right to have their data protected and control that data, but the GDPR explicitly says there are legitimate uses for the data and those should be balanced against the right to privacy.

The GDPR itself lists some of those balancing characteristics. It says specifically that uses such as network protection, identifying and preventing fraud, and reporting problems to law enforcement are legitimate uses. So, the law itself says the data can be used in this fashion. The challenge and the question is, "So, how do you balance those things and how do you do it?"

The idea of accredited access is that we have some sort of a framework private parties can use to look at the data. The general idea is this has to be a legal framework in which the parties are

bound legally to certain obligations and those obligations are going to be to honor the GDPR.

For example, in this kind of a framework, you're going to have to say why you're requesting a record and that should be recorded. It's going to have to have some requirements around data retention. The GDPR says you should only keep that data and have it for as long as you are using it and need to use it and then you should delete it.

So, those are the kinds of things that need to be worked into this kind of a framework, but the idea is have this framework, the parties are going to be legally bound to follow the rules. It also has to be auditable. So, that has to be part of the framework as well. So, we can't just say party X, you're now allowed to see the data. But we're also going to have to be able to go in and look at how they're doing their work, and if they're not doing it properly, there needs to be some penalties, such as you're going to lose access.

So, the GDPR actually talk about their accreditation frameworks. The problem is nobody has really gotten into actually building those and kind of shaping what they look like because it's something very new and there isn't a lot of experience. So, that's going to be some of the discussion that we could have in phase two. It's going to require some legal advice. There's some niceties

exactly around how the data can flow. There's going to need to be some sort of an accrediting body that reviews applications from researchers and reviews those accreditations on an ongoing basis and so forth.

So, GDPR seems to say we can do these things. The big question is what's the right balance? How do you actually make it happen, practically? How do you satisfy all the legal requirements?

But if we can get past those questions, we might have a solution that gives us some of the best of both worlds and honors what GDPR says we're supposed to do. Thanks.

JONATHAN ZUCK: Thanks. Yesim, can you go to the next of my slides, just quickly? We'll post these but there's two links in here that I used my own personal URL shortener, cpwg.wiki, to do. So, there's a column by Mueller that's talking about some of the data that Kathy and Farzi mentioned about some of these instances going down potentially and then there's also a link to under a block listing, a link to a blog that contains these two studies and the graphs associated with it. So, cpwg.wiki/blacklisting and cpwg.wiki/mueller are two reference points for some of the data that's being discussed. Do I need to spell his name? Milton. Yeah, your guy. He just recently

came out with a blog and made reference to the data that I think Kathy mentioned, so I wanted everybody to have it.

Do you guys want to take up some of this now? This was a lot of information. It's really new.

ALAN GREENBERG: Jonathan, your microphone.

FARZANEH BADII: So, there has been … I don't like the war of data and I have this much stats on … I mean, it can get factual, but also it can be like there's this company that comes out with this [inaudible] feature in 2018 after three months of GDPR actually reported that spam had gone down.

Now, there might be another company that after, because WHOIS was redacted, but still said that spam had not been affected, like the number had not surged up.

Then, there are other data that has been issued by other companies that say that, actually, phishing has gone down. But, as I said, I don't think that we should emphasize on surveys and data because then there will be a war. Then you will bring another source of numbers and if we cannot come to a conclusion …

The fact that … We need to revisit this in a year or two and see what the actual affect really is for an independent, neutral organization that has no stake.

So, I don't really think that these stats can help us resolve the issue because I also don't want to undermine the good work that security researchers do and say, okay, so the spam has gone down or has not changed because of WHOIS redaction, so we don't need …

The other … For example, on Farsight, and Paul Vixie once said that. He's a cybersecurity researcher, a very hardcore techie. He said that WHOIS might not actually been needed for tackling cybersecurity attacks in the future.

This is my personal opinion. Of course, that guy [inaudible] worked with him. But when we look at this data and these stats, we need to just look at them more objectively and kind of don't really take away too much from them and, say, on our side say that your work is not important. On your side, say that, oh, our work is really important, WHOIS is integral part of cybersecurity.

GREG AARON: I think the point is that in ICANN policy making we do need to rely on facts and data. We don't do it often enough, in my opinion. So, what we're doing now is we're starting to gather the data where

we can see, for instance, before and after. I don't think it's a good idea to necessarily try to kill the messengers in this case because the messengers have the data.

On one hand, we see that detection is down at some of these places. But if you look at the number of actual spam messages being sent on the Internet, it seems to be fairly constant. So, that says the activity is still taking place but we're not as good at seeing it in certain ways.

So, the data is important and you can't, I don't think, always impugn people's motives for gathering and analyzing the data. Thanks.

KATHY KLEIMAN: So, I did ask Jonathan ahead of time if there was anything we should review. So, I'd like to suggest that we all look at these data slides together and see – not now, but over time. And if there's a place to continue the discussion when we can look at the slides and evaluate them …

I did want to add, Elliot Noss, who is the President and co-founder of Tucows in Panama City, two-and-a-half months after the GDPR took place told us that one type of crime was down and that was the sending of millions of spam messages to registrants saying their domain names were expiring, because the WHOIS was

putting out the registrant's name, the domain name, and their registration date and expiration and millions of spam messages. I didn't realize it was that large. I was shocked when he told us. It had been going out to registrants. And those are almost non-existent now. So, he said that was way down.

Paul Vixie, I was at the speech. He's one of the creators of the DNS. He's one of the leading pioneers of DNS research and security now and he did declare the WHOIS to be obsolete and not needed for big types of DNS security research.

I'm going to throw a question to Laureen and Greg and to all of you and ask what is a cybersecurity researcher? And this is one of the problems is there's no credential on this one. So, one of the things we'll be needing and asking is: is there anybody who says they're a cybersecurity researcher? This is a problem we've had in the past. So, are we going to be checking for membership in groups like Anti-Phishing Working Group and others? And how are those groups going to hold their members accountable if there are problems?

GREG AARON: Okay. Thanks for the question, Kathy. SSAC also wrestled with this question. We wrote SSAC 101 which is getting into some of these issues and we talked about what's a security practitioner.

Basically, in our viewpoint, it's somebody who has some sort of a professional responsibility to deal with these problems but the question is even that might not be restrictive enough if we're going to be talking about access to the data.

I mean, access to the data comes with certain responsibilities, to be defined. Certain people or certain entities might not meet the level of responsibility and auditing and data handling that might be necessary for this.

The APWG was thinking about, well, could it become an accrediting body to examine its members? It knows who its members are and has relationships with them. But even then we figure not all of our members are going to have the capability to do these things properly and handle the data. So, we would have to come up with a long application process and an evaluation process to figure out who can really do this properly and then review their work on some sort of regular basis, and again billing and audit capability and that kind of thing. So, it's a broad group but the people who might be able to do this properly is going to be smaller.

COLLIN KURRE: Hi. My name is Collin Kurre and I just wanted to make a very short intervention because I hear what you're saying about the need to

have data and I just wanted to highlight some work that's coming out of the community to develop new impact assessment models that might be useful in this context when we're talking about tricky rights to security, rights to anonymity even, rights to privacy. So, I just wanted to highlight that and I'll post a link to the chat into this work and it might be useful for everyone here to have a more constructive dialogue. Thanks.

JONATHAN ZUCK: Yeah. The reason part of this is important is we need to have a discussion about whether we're going to give advice to the board [inaudible] and part of that is about the urgency of phase two and things, so that's where some of these things come into play. Olivier I think is next and then we probably need … We have Olivier, Hadia, Holly, Humberto, and Andrei and I may end the queue after that.

OLIVIER CREPIN-LEBLOND: Thank you very much, Jonathan. My question is actually I had in mind before it came on the screen. How much is registration data used to be able to qualify a domain name as being a source of spam or malware? I would have thought there are other ways such as using honeypots, such as a whole lot of other tools. So, perhaps is it time to rethink the way that we detect spam and

malware and so on, [inaudible] perhaps let me pronounce those words. I don't think we've used them yet – artificial intelligence. I'm not going to say we're going to use block chain, maybe not. But AI, who knows?

GREG AARON: Thanks for the question. WHOIS is one of the tools that's used but it's not the only tool and some of the other things … There's a whole set of scoring mechanisms that are used including what IP addresses are these domains sitting on.

One of the ways you find spam messages is through honeypots and then you look at what addresses are being advertised in the body of that mail because that's where the spammer wants you to go and those are the domains we really worry about, not the domain names that are [inaudible] so much but where they're trying to send you to because that's where the crime is going to occur.

So, you gather those, but again those are indicators sometimes of problems and then you want to find out what other domain names are also being used for that same scheme, because again, your goal is to prevent harm and do it as quickly as possible.

So, there's actually … The people who do this use a whole set of heuristics. They do a lot of correlation. They use some artificial intelligence. They don't use block chain.

OLIVIER CREPIN-LEBLOND: Here we go. I just lost my card, so now no more follow-ups afterwards. The DNS records have the data for the name servers and they also have the SOA record in there. Wouldn't that be enough to be able to establish a parallel?

GREG AARON: No. One reason is that a criminal will have their domain names set to a rather innocent-looking name server, like the default name sever that the registrar provides when you register the domain names. We don't want to block everything on those. There are a ton of innocent people using those. Then they'll switch their name servers when they're ready to start their criminal work. So, there's a switchover. And they know that because people are looking at the zone files and doing DNS queries.

They know what we do as well. This is a constant cat-and-mouse game. So, one of the things we're worried about now is because we've lost an important tool, are people going to start over-blocking or trying to compensate in other ways that might not be

a great idea? There are network operators who right now are starting to block entire TLDs. Any domain name from that TLD that comes through their network, they block it. That's not always a great idea. We still want universal acceptance and so forth but we're starting to see people move towards other solutions that might not be as precise and therefore might have some unintended affects of their own.

JONATHAN ZUCK: Thanks. Folks, let's limit ourselves to questions because we have our own internal debate about this another time. Let's take advantage of the panelists. Hadia?

HADIA ELMINIAWI: I had a question to Greg with regards to how much do you need historical data for your research purposes? Or do you actually meet any kind of historical data? Then, I just wanted to also reiterate what Greg said with regards to GDPR and legitimate interests.

JONATHAN ZUCK: Don't reiterate anything.

HADIA ELMINIAWI: Okay. I was just going to say that Article 48 of GDPR says that preventing fraud constitutes a legitimate interest and Article 50 also speaks about network security and information security. So, it's about historical data.

GREG AARON: Historical data is useful in certain in-depth investigations, especially when you're trying to figure out who is responsible. Law enforcement does that as well, and in some cases, we want to find out who the perpetrator is. That's important. The majority of things are happening in more real time, so the current data is really what we rely on.

JONATHAN ZUCK: Thanks. Holly?

HOLLY RAICHE: Really, a couple of questions. First of all, the way you've described what you do, it is potentially criminal but it may not be criminal and I'm thinking of a GDPR definition of law enforcement agencies and whether you fit and I think that's my first question.

In terms of the sorts of exceptions as to who can get access to data and what's being talked about as law enforcement agencies, what kind of definition that's broad enough to get both of you

with enough protection around the data that both of you get to address Kathy's issues as well. In other words, what is the definition? How do you fit into a possible exception as to who should not get data? Because the terminology I've been hearing for a long time is law enforcement agencies.

Now, to me, law enforcement agencies [inaudible] agencies that's responsible for breaking the law on this would include [inaudible], consumer, and so forth. I'm not necessarily clear that that's the way GDPR is interpreted.

I'm also not clear that that's the way what he's talking about is interpreted. In terms of how do you do define that as an exception and what rules do you ride around that? Kathy is actually smiling.

JONATHAN ZUCK: I'm sorry, lots going around behind me. If I can break your question down a little bit, I think you're asking that given the exceptions that we're talking about – fraud prevention, etc. – do you believe that the GDPR leaves room for non law enforcement actors acting in those interests to participate?

GREG AARON: As I mentioned, a lot of these functions are not the functions of law enforcement to begin with. The protection of networks is not

a law enforcement function. It's the function of the people who are owning an operating the network. Law enforcement may pursue fraudsters, but a bank, for example, needs to understand who its customers are, needs to be able to process payments—

JONATHAN ZUCK: Sorry to just cut you off. Do you think that GDPR understands that distinction? In other words, are we as the At-Large or other [inaudible] going to need to fight for your position in that exemption? That's the question.

GREG AARON: I think it's pretty clear and pretty explicit that it was written specifically to allow access by [inaudible] other than GDPR. Let's remember GDPR, there are separate and parallel laws for law enforcement, for dealing with the privacy laws as well. The role of [inaudible] I think is pretty clear.

LAUREEN KAPIN: Right. And to put it even more simply, law enforcement are not the only third parties who have the ability to apply for access under the GDPR.

HOLLY RAICHE: I'm going to ask Jonathan to actually interpret what I'm saying because I don't think you've answered my question.

JONATHAN ZUCK: I think we'll take it offline. I think he did but we'll talk about it. He believes the GDPR does account for non law enforcement actors. So, that's his answer to you question. But let's keep this going. I wanted to get to Humberto before we lose translation in particular.

HUMBERTO CARRASCO: I'm going to be very brief in my question. This is a brief question and a comment. It seems that there is a contrast between these two positions from the left and ride sides, particularly when it comes to data and I believe there is a mistake in the point of view because perhaps Kathy mentioned some information regarding a decrease in phishing and also a decrease in the amount of spam perhaps, since the GDPR is effective.

But on the other hand, there is a complaint by Greg, if you will, because there is certain impossibility to access data, so I believe that this is a preventive aspect from the situation. There is a decrease in number because we are not able to access data. Otherwise, once the crime is committed – the supposed crime is committed – we are not able to access the information but that is

a reaction, so that's why I believe that there is an issue here because we are discussing different aspects in the same line and that might be a mistake.

JONATHAN ZUCK: I'm going to give the last word to Andrei.

ANDREI KOLESNIKOV: Thanks. My daughter works for the private company which is dealing with spam and scam and all this stuff and she's dealing with the registrars on a daily basis. Just a little portrait. The average age is 25 years. So, it's a young guy, young girls and boys, sitting with the Internet protecting everybody from various dangerous things. But the customers are banks, airline companies, insurance companies, big brands, small brands. What they do, they daily have to deal with WHOIS and thanks to the American registrars because the WHOIS data is still up and running and most of the requests … It's interesting. It's Russian companies but the Russian part of it which easily can be resolved with the Russian registrars and most of the – 8% of the requests goes to GoDaddy and big registrars in America. What they basically do, they bring down the bad domains. It's pretty much going okay but they already see the impact of the changes

because the reaction became slower. The reaction time increases.

So, it's not very … I should not say everything fell apart but they see the difference. It's already there. Just a little facts.

KATHY KLEIMAN: That's a fair observation, of course. The reaction time is slower because the registrars, under GDPR, have to evaluate both the need of the requestor and the rights of the registrant, so there's actually a human intervention. Olivier, we don't have the AI on this yet, but I'm sure they're working on it.

So, by definition, it's not automatic anymore. It's not an open database. It has to be slower. Hopefully, it will speed up as humans get used to it and create more automated types of systems and I think that's what we're talking about with some of the access.

FARZANEH BADII: The requestor has to be held accountable and those [inaudible].

ANDREI KOLESNIKOV: These are official letters, signed, names, what companies, what subject.

FARZANEH BADII: Yeah, but we have no [inaudible] that mechanisms were of course expedited. Urgent answers will be done when those accountable to mechanisms are in place.

JONATHAN ZUCK: Okay. So, we've unfortunately run out of time on a topic that others have spent half of their lives on for the past couple of years. It was a challenge to being with but I really want to ask you to join me in thanking the panelists for showing up and being civil to each other and everything like that. Thank you so much. We have a lot of conversations to go forward including one soon that Alan wants to run about what we should do next on EPDP. So, we have a little more information in front of us now and I really appreciate the folks that came up to help give us some more data.

FARZANEH BADII: Thank you. I just really appreciate this invitation. It's really important for us to have a collegial relation with At-Large and that you include our perspective here. It really means a lot. Thank you.

JONATHAN ZUCK: [inaudible]. Thank you. So, thanks for the tech support staff, the translators for staying late. We really appreciate it. For everyone else, go eat.

UNIDENTIFIED MALE: As master of the clock here, the next session is starting at 12:15. It is 12:10 now, so we are not going to give the full 15-minute transition break. Lunch and the At-Large Leadership working lunch begins at 12:15. So, don't go out and loiter. Stay here and eat and work.

[END OF TRANSCRIPTION]