BARCELONA – GAC Public Safety Working Group Meeting
Tuesday, October 23, 2018 – 08:30 to 09:30 CEST
ICANN63 | Barcelona, Spain

LAUREEN KAPIN: Good morning. A special thanks to everyone who is here bright and early to join us for the Public Safety Working Group meeting. We're going to get started. If folks have questions about topics, please feel free to raise your hand and we will take your question.

I want to just briefly introduce my colleagues at the table. To my right is Fabien who is from ICANN staff and provides countless hours of devotion and dedicated support to our team. We're very appreciative of that. We really couldn't do our work without his great energy and support. To my left, I'm going to let folks introduce themselves.

GREGORY MOUNIER: Good morning. Thank you, Laureen. My name is Greg Mounier. I'm working for Europol.

UNIDENTIFIED SPEAKER: Good morning, [inaudible] European Commission, DG Migration, and Home Affairs, working on the fight against cybercrime.

IRANGA KAHANGAMA: Morning. My name is Iranga. I'm with the Federal Bureau of Investigation in the U.S.

CHRIS LEWIS EVANS: Good morning, my name is Chris Lewis-Evans and I'm with the National Crime Agency of the UK.

LAUREEN KAPIN: And I'm Laureen Kapin. I co-chair the Public Safety Working Group with my European Commissioner colleague, Cathrin Bauer-Bulst, who will be joining us later today, but not this morning. And I am from the United States Federal Trade Commission where I focus on consumer protection matters.

Next slide, please. Sorry. Next slide, please. So we're going to give a brief overview of our Public Safety Working Group activities. We're going to be devoting most of our discussion to WHOIS and compliance with GDPR. And the impact of the very significant changes on the availability of the WHOIS, both in terms of availability itself and the content that's now available, how that has impacted law enforcement. And then finally, we're going to wrap up with some information and updates about the Domain Abuse Activity Reporting, also known as DAAR. And we're very pleased to have John Crain from ICANN join us, who's right there at the end of the table.

So with that, we're going to get started on the substance. Next slide, please. So we have several strategic goals in the Public Safety Working Group and they're on the screen before you. To develop

antiDNS abuse and cybercrime capabilities, cybercrime mitigation capabilities. We want to preserve and improve the domain registry directory service effectiveness.

And, by the way, the GDPR actually has requirements for accuracy of WHOIS information, which hopefully will be another tool in our toolbox to continue to advocate not only that the information should be accurate, but now that there are actual legal tools to enforce the fact that that information should be accurate and that's a plus under the GDPR.

We also want to make sure our own group is robust and effective. So we want to encourage participation from a diverse set of folks from around the world and in different law enforcement and consumer protection public safety agencies. And we're constantly trying to get more people into the fold. So if anyone out there is interested, please come speak to us.

And then finally, we want to develop participation in Public Safety Working Group work and ensure that we hear from our stakeholders, we have regular meetings with different stakeholders around the community during ICANN meetings, and sometimes intersessionally. And if any stakeholder groups would like to meet with us to have a discussion that is a little bit smaller than the whole GAC room, please reach out to us. We're happy to meet with you.

So now we're going to focus on number 2, the WHOIS and GDPR issues. So among the many work streams that are going on is the RDS2 Review Team work. That's the review team tasked with looking

at the registration directory services system. And their goal was to find out more about how WHOIS is used, whether it meets investigative needs of the users. And also, and this is very significant, to provide a first look about the impact of the changes post-May 25th when the temporary specification went into effect.

And the review team launched a survey with very specific and relevant questions about the impact of the temporary specification and the changes, the drastic changes to the WHOIS, how that has impacted users. There were 55 respondents from many countries. They are listed on the slide, but from A to Z, Australia to Zambia, so this was rather a robust participation.

I am going to go through some of the results because they're especially pertinent. And I would urge you all to look at these at these slides also at your leisure. Again, because they contain very significant information. So Frequency of Use - how often did your unit use the WHOIS prior to May 2018. So you see the biggest category here between 100-1,000. That is the biggest category. And we also have between 1,000-10,000, fairly large.

And sometimes there's an I don't know. And I do want to highlight the I don't know, because it's actually sometimes very difficult for law enforcement agencies to be able to track that information because so many users within the agency use WHOIS, but it may not be very easy to get those users to actually take count and measure. So there is still a lot we don't know. But what we do know is that before May 25th, these categories between 100-1,000 is the largest category.

So here we have a comparison, a sort of before and after comparison. Did WHOIS meet investigative needs before May 2018? And you see our largest category in the green is yes. So that's 53 percent. And then a partially at 45 percent.

But look at the next slide, and we see that that yes, it had been a little more than half of the pie, now that is reduced significantly from 53 percent to 8 percent. And the no, which had been a tiny little sliver of the pie, that has increased drastically to about three-quarters of the pie, 67 percent. That's signified by the yellow area. So that's a huge difference between pre-May 25th and post-May 25th. And the takeaway there, at least from these respondents, is that the current WHOIS, the one that exists now, does not meet investigative needs.

What is the impact of unavailability? Here we have two questions. Are there alternatives that you can use for your investigation? So the yes category is about 24 percent. The no category is the largest category. No, 60 percent say no, that there isn't a great substitute for the WHOIS.

Moving on to the right hand pie, what is the impact of the lack of this information? What is the impact? So the biggest impact - and this is a takeaway that we've also heard in our informal Public Safety Working Group meeting yesterday where we had a group of a diverse set of law enforcement folks around the table. Folks were from cybersecurity, from folks focusing on child abuse, folks from consumer protection, a variety of places. And the 201 really all emphasized the biggest impact is that the investigation is delayed. The investigation is delayed. It takes longer to investigate these crimes. And some of them are very

serious crimes where people are at risk of physical harm, financial harm, etcetera. So those investigations are delayed which often means that then the harms continue.

And I also want to note that another big category here is that the investigation is discontinued. And that is almost 26 percent as an impact. So those are serious impacts. Impact on Cybersecurity. And that is an issue, of course, that is corely something that ICANN and the community cares about. The security of the DNS, that is a core part of ICANN's mission and mandate to keep things secure in the domain name system. So again, we have a lot of serious issues here. How do you use WHOIS query data? So this sort of lays the foundation. Cybersecurity folks use WHOIS data to identify cyber attacks. That is our largest category, almost 90 percent.

And then we have another series of issues that are related to cybersecurity. So to figure out what domains are related to that attack, to ask for assistance from the registries, registrars, web hosts, etcetera, so that they can get help in stopping that attack, to compile block lists. These are the reputation lists that tell us who the bad actors may be. And then also for IP purposes or other business or legal purposes.

Next slide, please. So here is the impact on cybersecurity. And again, this is a very important highlight. This sets up the fact that much important WHOIS data is currently redacted, i.e., that means it's not available when you do a WHOIS lookup. You will not see certain personally identifiable information, like the name of the person who is

associated with that domain name, like their email address, for example.

So this asks a very important question, which is when an investigator does a WHOIS lookup and they are finding that certain information is redacted, is hidden, is not there, this is asking have you submitted request to reveal this redacted WHOIS information? And there's supposed to be a system for doing this. In fact, that's in the temporary specification, that there is a requirement that there be a way to request this redacted information. But we see here that there's a real significant knowledge gap.

So our biggest category is when people are asked, have you submitted a request to get this information that's hidden? Our biggest category here is, I don't know how to do this. I don't know how to do this. And, of course if law enforcement investigators don't know how to do this and cybersecurity researchers, who one would think that these would be the folks who would be most interested, who would most need to do it, if even they don't know how to do it, then that shows that there's a real significant problem here.

And then we just have the other categories, no, they haven't submitted a request, and some folks a little under 20 percent, have submitted requests.

Here we have again impact in terms of what happens when you do submit a request. Our largest category, most troublingly on the cybersecurity issues, is that they have been denied access with no explanation. It's a little bit over 50 percent.

The second category denied access and told to seek a court order. And I want to emphasize there that seeking a court order is no easy thing. You actually have to have a significant amount of information to even be able to go to court because you have to make your showing that that court order is justified. And there's sort of a Catch 22 here because often people are seeking information within the WHOIS as a first step. I need that information so I can go to that source and get more information so that I could then make a showing for a law enforcement investigation or proceeding in court. So if you can't even get through step 1, you are really cut off at the knees.

And then also I do want to emphasize that some people have been granted access and that's a good thing. That's a little bit over 30 percent.

This goes to timing issues. When you were granted access, how long did you have to wait, essentially? And here actually, a little bit of good news. Within seven days. That's our largest category. Longer than seven days is a little over 25 percent. Within seven days is almost 40 percent. So that actually is fairly quick. For that smaller group people from the previous slide that got access, they got that within seven days. So that is a bright spot here.

So here, it's a series of statements in answer to this question. Which of these statements best matches how the changes introduced in the temporary specification affected your investigation? So let's look again at our biggest category in red - our investigations are affected. We have not found alternative data sources and our time to respond

exceeds an acceptable threat threshold. And that's about 65 percent. That is the statement that best matches the impact here. So again, that's a very significant impact.

I do want to note that the category in green at the bottom, our investigations are unaffected, that is only, just doing a rough guesstimate here, that looks to me to be about 3 or 4 percent. So that's a very, very small piece of the pie here that is unaffected. Everyone else is affected.

This again is more variations on the theme that the experience with the temporary spec in terms of redaction, it impairs or delays our ability to conduct searches to attribute abuse to actors. And that's our largest category here, over 70 percent. And when we say attribute, that basically means connecting the illegal act with who is doing it. And that is one of the key things you want to do with searching for the WHOIS data. If there's a domain involved, you want to find out who is behind it so you can then use that information to eventually get to who is responsible for the bad acts.

Here we have what, if any, issues do you have with the temporary specification and how it's altered the WHOIS? And the biggest issue that's identified is that redaction is excessive and that's over 90 percent.

And this drills down into the notion that the temporary specification can be viewed as going beyond what the law requires, going beyond what the GDPR requires. And here the two biggest categories are

redacting legal entities is excessive. I want to drill down there a little bit.

The GDPR protects personal information. That's information that relates to a person. It does not protect information that relates to a legal entity. So corporations' information is not protected, yet the temporary specification does not make that distinction. And there are some nuances here. Sometimes legal entities can disclose the information of a natural person. So again, there is some nuances, but the temporary specification doesn't make those nuances, and it goes beyond what the GDPR requires.

And then there's also a territorial issue. There's a very specific extraterritorial -- when I say extraterritorial, I mean beyond the EU borders breadth of the GDPR. But it does have limits. And again, there is a view here that redacting, that the redaction currently taking place goes beyond what the GDPR requires. That's our other high category of information.

So I'm going to move here to a different topic. We've looked at some very significant survey results conducted by the review team tasked with looking at the WHOIS system to date. And that survey was very significant because it had so many respondents and the information was so specific. But now I also want to turn to discussions that we had yesterday with a really great group of law enforcement folks around the table who come to the ICANN meeting to grapple with these issues. And they talked about some real-world impact on law

enforcement. I'm going to turn this discussion over to my colleague, Greg Mounier.

GREGORY MOUNIER: Thank you, Laureen. Good morning. So yes, this is really a slide to sum up a little bit some of the conclusions we had, the discussion we had with colleagues from the law enforcement community. And also the feedback we've been having for the last five months. Five months, why? Because this is when the temp specs have been starting to be implemented. So now we start to have a bit of a historical perspective on the impact we have.

And in addition to the excellent survey that Laureen has been telling you about, I think we've got a number of key points that are essential for us to tell you about. One of those is in the temporary specifications you've got Annex A Section 4 which kind of provides a framework for the contracted parties to disclose information without a court order to investigators, and law enforcement, and the judiciary.

And so we have said almost since the beginning in the Public Safety Working Group that we thought this, and in the GAC, that this section was not clear enough, wasn't providing clear guidance on how to implement those disclosure obligations. And five months later, we have come to the conclusion that we were right indeed, and there's really a lack of preciseness and guidance for the contracted parties to actually deliver on this provision.

And so what we see is that for those law enforcement people who know that there is a possibility to request information that is now nonpublic, then when they make requests, we see that the result is very unpredictable. Sometimes they get the information. Sometimes they just get a systematic no, I want a court order, which is a very restrictive reading of the Annex A Section 4. But it's very inconsistent. And we're not blaming anybody really. I think it's the lack of clarity, the lack of guidance in each section which has this negative impact. So it's still vague.

And then when you make the requests, you don't know what you get. It puts really the contracted parties in a situation where they for very understandable reasons, have to make a call whether they need to protect themselves in terms of liability. And so most often, they will take a very restrictive and conservative approach which is not in the spirit of the temporary specification we think. And the fact that some are requiring systematically court order is definitely not in the spirit of the temporary specification. So there is really a need here to clarify the framework in which we are making those requests.

The impact of course - and that's what we see on a daily basis, is that investigations are taking longer. What does that mean in practice? If you are investigating a scam, it will take longer for you to identify the perpetrators who have set up this malicious website running the scam. And that means that victims are being victimized longer. I mean, relate that concretely to somebody, your grandmother who's been victim of a scam, and then because it will take longer to get the information, she will continue to be abused longer and there will be

more victims. That's how we see it from our side and this is really distressing for us, I think. And I think I really want to emphasize this aspect.

And we don't see the full impact yet on investigations. Why? Because often when you speak to investigators not really privy so ICANN, they say, no, that's okay. We've got this super subscription to this third party tool that gives me access to all [inaudible 00:26:31] information. Yes, of course. But the effectiveness of that tool is degrading. We know that because every single registration made after the 25th of May is not in that database. So you might think that you can do your investigations based on that tool, but in fact, you don't know what you don't know because all the new registrations are not in that database.

So there is a time gap. It's difficult for us to tell you, yes, as of the 25th of May, I can't do any investigation anymore. No, it's not true. I just do my investigations, but because I don't know what I don't know, then I think I'm fine. In fact, you're missing out a lot. And I think that the more time will pass, the greater the effect will be. So the ability to attribute crime is really degrading.

CHRIS LEWIS EVANS: And just to give you a sort of real-world example that we had yesterday on this. So one of the investigations that we were running, we were notified of 200 domains that were suspected of committing business email compromises. So this is where someone uses a domain name that looks very similar to an actual one and then will contact the head financial officer or someone below and pretend to be the head

financial officer, to try and fraudulently attain funds from that company.

So we received those 200 domains. Obviously, under the old WHOIS, we would have been able to very quickly identify contact details for every single one of those and verify those. But instead of this, we obviously had to send some emails out for some of these to test the waters. We weren't able to obtain access to any of the registrant details for this. We were asked to provide court orders for each of those.

So at this point, that's not reasonable for us to go out and get a court order from a number of different registrars and then access this data when we've got people that we know are at risk of financial loss. So this had an impact of tying up two or three investigators having to do background checks on suspected company names and trying to work out whether that was the company at risk.

So a very - as you can imagine, all businesses and law enforcement are very tight on resources So this act of having to do extra work and extra background research takes a lot of that time and stops them doing their other very important work. So in one of the cases, we did all this research, we contacted them, and we heard back from them that thank you very much. Yes, we have received an email trying to obtain 50,000 pounds from us.

Luckily, someone had spotted it, but that had happened before we were able to contact them. Had they not spotted it internally as a fraud, that business could have lost 50,000 pounds just from the delay

that was built into us not being able to get access to timely data. So it is important that we do have a system and the contracted parties are given the backup and the reassurance that they can legally provide us that data. Thank you.

GREGORY MOUNIER: Thank you, Chris. Next slide, then. So really, if we could sum up a little bit what the law enforcement community and the judiciary would need in the next system, which is an essential piece of accountability online. I really have to stress this. First of all, we really need to build a system that gives immediate access to nonpublic data via a central portal. This is why we tend to support enthusiastically the idea of potentially having a unified access model. For us, I think it's definitely the way forward.

As Chris explained, the way you investigate in the 21st century, criminal activities online, require that you have immediate access to this type of information. You can't buy the argument that we have an international system based on [inaudible] and that we can apply a 19th century judicial corporation tool to the 21st century in a digitized world where everything goes very, very fast. You can't be waiting for nine months to get evidence. And I think it has to be said very clearly. So that's the main requirement.

Now, reverse lookup. We know that this is contentious. We know that we've understood the argument that this was not an original feature of the WHOIS. We take it. But I think it's important to make the points that amongst all the features of the tools that we have currently and

that we used to have in the former WHOIS, the reverse lookup is probably the most important feature that investigators are using.

So for those who don't really understand what the reverse lookup is, when you make your WHOIS look up, you make the lookup on the domain name and then you see the information and the registrant. When you do a reverse lookup, you take any of these identifiers, so it can be an email address, it can be a name, can be a phone number, and then you search the database, and then you get the connections of all the other domains that are connected to that identifier. And this is really, I'm being very blunt here. You can ask all the investigators here. This is the most important feature.

So whatever system we come up with, it has to be GDPR compliant and we're convinced that within the GDPR there is the right legal base to balance privacy and security. We need to be able to be on that feature. At least for law enforcement, this is absolutely essential. Historical WHOIS -- same. We need to have the historical perspective.

Sometimes domains are being registered in bulk by criminals. They will just park, and at some point, they will use it for perfectly legal activity. And then they will remove it. And then they will use it again for more criminal activity. But you need to be able to look into the history of the domains in order to find the information you need and make connections. That leads us to think that we need to have a proper discussion on the data retention period. We can't be too conservative. We can't just say, you know, six months after the end of

the life of domain. That's not enough. Honestly, we have to balance the needs of the investigators to what will be in the new system.

Single and multiple query capabilities. Of course, having the ability to search a domain in the database is essential. But more often than not, when you do an investigation for instance in a [inaudible] or other criminal infrastructure that's based on domain, you would need to do multiple queries. I don't want to use the b-word, but you need to do a lot of queries. And this is just a fact. And again, we believe that within GDPR and data protection legal framework there are exceptions for legitimate actors. And we believe that we can make the argument that this is necessary just because this is a fact of life. If you investigate criminal activity online you need to be able to do massive queries.

Cybersecurity researchers have to have access to nonpublic data. Cybersecurity is a matter for everyone and we're not alone. In fact, the public investigators, the police has very limited resources and our work is done partly because a lot of the people in the private sector are working on it, giving us tips, and we're all in it together.

I can give you an example of an investigation that Europe was coordinating with a number of American agencies in the field of counterfeited goods and the rest. And we do that for about nine years now, I think. I'm looking at my colleagues. Even longer now. And we do it regularly every year and we take down a number of websites that are distributing counterfeit medicines, counterfeit goods that have a strong impact on public health.

And this year, we're still expecting the result in the coming months, but we can anticipate, but because of the fact that our colleagues in the private sector do not have access to newly registered domains, the result of that operations probably for the first time in seven years, will be not as good as it was last year. I can't comment more on that, but we will probably communicate in a few months on this operation. And this is really a concrete example of redactions of WHOIS information. Thank you.

LAUREEN KAPIN: Thank you, Greg. Next slide, please. So Iranga, I would love for you to introduce our guest, John Crain, to talk about the domain abuse activity reporting system aka DAAR.

IRANGA KAHANGAMA: Sure, thanks, Laureen. And I think that Greg's last point is a really good transition to John Crain, to emphasize the relation between cybersecurity researcher and law enforcement. Kind of how you see John on stage with us now. Because that is really a big aspect of this. One anecdote that I've always heard that I think is a very good reference, from the United States at least, if you can go to US doj.gov right now and our Department of Justice lists a number of indictments and criminal charges against cyber criminals that we do.

And if you read those throughout the press releases there are a number of companies that are always listed at the bottom. And a lot of them are private cybersecurity firms who have provided data and

were really a lot of the eyes and ears for us because of our limited capabilities and resources. So I just wanted to kind of mention that to emphasize the need to work with cybersecurity and to enable those types of groups.

So that being said, I would like to introduce very briefly John Crain with ICANN security. I think he's given this presentation to us a few times. We've had calls and had him out at least in DC. So he's going to give a few minutes on the domain activity abuse reporting tool. I know there have been some updates. He had some studies conducted about the sources.

And I guess specifically too, looking at how any of the impacts in WHOIS you're seeing are affecting some of the tools and lists that may be sources for DAAR. And then additionally, given that you are in a room full of government representatives, maybe speaking how something like DAAR could be applied to these respective government agencies, their missions, and helping them ensure public safety within their own countries as well. Thanks.

JOHN CRAIN: Thank you, Iranga. Let's get the slides. So the main abuse activity reporting system, commonly known as DAAR, which is not the best acronym in the world, what it's basically doing is it's measuring reports of abuse in the domain name system across the generic TLD space. And what this allows us to do is to build a picture of the threat landscape and to see how malicious actors are actually abusing the system.

Many of you may have already seen this slide so this is a shorter version. I will be giving a longer 90-minute presentation tomorrow. It's different to some of the other tools that out there in that we are looking at a wider space. There are other people that have developed similar tools. This is not rocket science. It is not something that we invented ourselves. It's based on studies and previous work that is out there. But we study across the entire generic TLD space We're using a large set of reputation lists. Those are the feeds that people use in firewalls, etcetera to protect their networks. And we're also saving that data so that eventually we'll be able to do some interesting historical studies.

At the moment we have about two years of data which is more than we had two years ago, but it's not enough to do really long-term trending yet. But the hope is in the future we will be able to. And it studies some very specific threat types, phishing, bot net command and controls, malware, and spam. And the reason we pick those four is because these are things that actually came out of advice from the government advisory committee over the years. And they've been clearly identified as being abuses we should look at. And basically, we're trying to take a scientific approach to this. We're trying to be as transparent as possible.

When dealing with security data that, of course, has some issues, but we're being as transparent as we possibly can. But most importantly, we're trying to do it in a way that is reproducible so that others, for example maybe law enforcement agencies or private security

companies or academics, can actually take our work and use it to build new tools. Next slide, please.

So what could you actually use this data for if you had it? Obviously, you can report on threat activity. You can see the changes day by day and you can see how things affect the threat landscape. You could, of course, study histories of security threats. You can also, of course, study history of how policy changes may affect things. We can use this to help the operators understand how to manage their reputations because a lot of this is reputational data. This is what is out there in the public domain.

The real key reason we built this was so that we could help other communities understand the ecosystem and that we can actually inform the policy discussion with data. There is a lot of anecdotal evidence and there's a lot of discussion about things are getting worse, things are getting better, often at the same time depending on who you talk to. The data is what it is. We try not to make opinions or our own views of what the data means. We try just to show the data and let it speak for itself.

So the way we do this is basically we conduct all the gTLD zones. We can collect about 99 percent of them through the centralized zone database system that ICANN runs. We use publicly available methods to collect that zone data, as I said. We only look at the domains that appear in those zones on a specific day.

The reason we do that is because we're trying to get an idea of the threat landscape. And there are many names that actually never get

registered and never get used. And until they're registered and actually resolving, they're not really a threat at the moment. We could have lots of discussions about whether you do the whole zone or you do the whole registration system, but if anybody has actually tried to collect the data on all the registrations, it's not out there publicly. The zone files you can get. So we're really trying to do this with publicly available data. Otherwise, it wouldn't be replicatable.

Currently, we are looking at about 1240 gTLD's, which is the majority of them. And we're looking about - actually, I looked this morning, 196 million resolving domain names. So we count the unique abuse names. So we count names in two ways. We count by each category of threat where a name was used for that. But then also we de-duplicate and just count the name a single time as an abuse name.

So a name can be an abuse name only once, but it can also be counted in multiple categories. Because sometimes a phish is also involved in spam and also involved in malware. So sometimes you will get a name that is used for multiple things. So we do map that. But when we count a name as abusive, we only count it once.

We use multiple feeds of reputation data, otherwise known as block lists. I will publish the list in a second of what we use. We de-duplicate and we do some magic math on it and then we produce numbers. The numbers basically tell you how many names is in a specific zone, how many of those have been listed as being abusive, and the types of abuse they've been listed for.

What DAAR does is it actually reflects how the community that is protecting the end users sees the DNS system. Because these are all names that are actually in use in lists. An important part about that is we don't create our own reputation lists. We make no decision one way or the other as to whether a name should be on a list or should not be on a list. It is either there or it is not. This is the same abuse data, as I said already, that is used throughout the security industry and also throughout many academic studies.

So as I said, we don't make opinions on the data, we don't edit the data to decide what is and is not abuse. We just gather data and publish it. Does DAAR identify all of the abuse? Well no, we're only looking at particular types of abuse. We're only looking in the generic TLD space. And we are only looking at things that are being used by the security industry. So it is a limited view, but nonetheless, it is very interesting. And the techniques could be used for a wider view. You could use more or different reputation feeds. You could look at a wider range of TLDs.

So this is the list of reputation feeds we use at the moment. There's quite a lot of them. Malware patrol has a lot of sublists that we use. I'm not going to go into this in detail, but we have the slides and you can look at them. It's a question people ask us is which lists are you using.

So this is just a partial list of some of the academic studies and citations that we used when deciding which reputation block list to use. And there are many more. Basically, what I'm letting you know

here is this is quite well-documented science. It's not something we just made up.

So where are we? Well, good news. My favorite piece of news is I've actually just hired a new researcher to work on this. I think somebody mentioned something about resources. We have the same problem. So as [inaudible] joined us October 1st. She's reasonably well-known student, an academic, that has just got her PhD and is quite well published in the area of abuse and identifiers. So a very welcome addition to our team, and she will be focusing on identifier abuse and, of course, the DAAR system. And I'm hoping to be able to bring her with us to Kobe so that you can meet her and have discussions with her. But she's only been with us a few weeks and I thought it would be a little bit cruel to put her in front of the community on those first days.

So we took the methodology, we wrote it up, we published it, and we gave it to two independent reviewers. We paid them to do the review, but they were left completely independent. And then we posted both the methodology and those reviews for comment. The comments were to DAAR at ICANN.org. We did through an email system rather than through the public comments system which is very - although much more transparent, is not something that many security folks want to use.

So we have a lot of - well not a lot, we only got five comments, but some of them will be redacted when we publish them because the people do not want to be identified. Anybody who works in the

security industry will understand that there is risk with the work. There's a link there if you want to read it.

We only got five comments, one of which was published by the registry stakeholder group. The other four we are communicating with the commenters to see how comfortable they are with us publishing their names versus the actual comments themselves. We're assessing those comments. There's a lot of them. And we are going to publish the answers to each comment or question in written form by December 1st. My hope is to do it before then, but I'm committing to December 1st because it is a lot.

Some of the comments are highly technical. We will try and break down the comments to things that we can manage right now. Some of them have actually already been addressed. And to those that we will address in the future and those that we just don't think are relevant to the methodology discussion, and that will be by December 1st.

We are going to start publishing monthly reports. I'm committing to the beginning of 2019 because really we want to get the review thing past us. We actually have draft reports. They are ready to go. We will backdate the reports. So we will do some of the older reports so that people can see the change. These will be monthly snapshots of the data with monthly deltas so we can see some change.

We are still investigating whether or not we can publish the specific data with a specific strings of TLD's into the open data initiative. We're not there yet. We're still discussing that. And, of course, we're also

going to continue coming to ICANN meetings and other venues and talking about the content of the data when we get here.

Something that I've been doing in the last few months is talking to registries. We're very comfortable with our registry data. We're a little less comfortable with the registrar data and we can talk about that in tomorrow's event. So we are reaching out to registries, and more importantly, they are reaching out to us so that we can have peer-to-peer discussions about what we are seeing versus what they are seeing. And this is turning out to be quite useful. When a particular registry goes and adapts their processes to deal with a particular type of abuse, we can actually see that in DAAR. If they're affected by a particular attack or a particular misuse where they get more abuse, we can also see that.

So we do that not as ICANN's compliance team or from a compliance standpoint. But we really try and do that from a interested security practitioners, peer-to-peer, so that we can try and solve some of the problem. We've already had a lot of very good constructive data-driven discussions with industry members and we are continuing to have more.

We're open to that discussion. We want to figure out how else we can use the data. There are sets of that data that are limited by such things as our contracts with the data providers where we can't just pass on the feed. But some of the derivative data we can publish. And the question is, what is the best way to publish that? Where should we best publish that? And how can that be used to inform the

discussions? Although the comment period finished a while ago, if you have comments, don't hesitate date to use DAAR at ICANN.org to send them. This is going to be an ongoing project for many years. And at any point, if you have good suggestions about how we can improve it or you find issues with it, please write to us and let us know.

As I said, I will give a broader update tomorrow, room 127 in the afternoon. So if you have in-depth discussions about DAAR, you might want to save them until then when we have more time, but I'm happy to take them here too. Thank you.

LAUREEN KAPIN: Thank you, John. So we have a very brief time for questions, but if folks have questions now is the time. Kavouss, I see you first.

KAVOUSS ARASTEH: Thank you very much, and thanks to people on the podium, yourself, Laureen, that I know, and Chris also that I know, and also special thanks to Fabien. They're really helping, from the ICANN point of view, the governments relating to this very, very important issue. It's top priority for us and for everyone else. But sometimes we should look outside the paradise. Outside the paradise are those areas that some developing countries, they are living and they don't know what is the situation at all.

So I think we need to take on board this issue. I request you, Laureen, when you present your report, it should be in the communique the situation drawing the specific and special attention of the GAC

members and even those who are not a member of the GAC government and so on, so forth, to look at these very, very important issues.

Now, what you have mentioned, there are two different categories, categories relating to the EPDP. You should take it up your member or alternate by a member to others and you have to raise the issues and I would be very happy to further discuss this issue. But this is important, however, we are very limited in the EPDP team. We are three only and there are another 26, and that 26 should be convinced sometimes. They are inconvincible to agree with us.

The other issue is that have you or do we know that a sort of statistic asking countries, question one, do you know what is WHOIS? Yes. Do you know how to use is it, yes or no? Have you used it, yes or no? Have you faced any problems or difficulties, yes or no? If yes, what are those difficulties and so on, so forth. We need to really launch something to bring the attention of the countries that they may not know. I'm not saying that every country doesn't know that. Many may know, but many others may not know.

And I think this is a very important issue and perhaps one of the elements mentioned that I understand the gentleman from the EUROPOL or INTERPOL? Doesn't matter, pol is pol, saying a lot of problem has been created. Is it because of the GDPR? Is it because of the temporary specification? If it is because of the GDPR, we can't do anything about that. If it is because of the temporary specification, yes, we have another five or six months to push for that. I'm sorry to

remove some of the difficulties mentioned in Annex A and so on and so forth, but for the time being, put GDPR and the temporary specification out.

Did you have the same difficulty before? If yes, what have you done up until now? And what does GDPR bring to that? Does it resolve some of the problem that you had, yes or no? And if it does, what about the temporary specification? Does it make the GDPR more difficult to implement or less difficult to implement? These are the issues that we have to know. At least as a member of the EPDP, we would like to know what are our next mission in the group? what we have to react? How we have to react? What point we have to take? And we need guidance from GAC and we need that you kindly include that in your report.

So by the way, thank you to all the people on the podium. They were one of the most useful presentations and I appreciate all of you. That was very, at least for me, it was learning of the process, and I got many things from that. But I think the issue requires very careful consideration and attention. Sorry, I was long, but I had to raise this point. Thank you.

LAUREEN KAPIN: Thank you, Kavouss. I think I also saw the United States in the queue.

UNITED STATES: Thank you. Ashley Heineman with the US. I just wanted to ask even if just anecdotally through the effort of the survey, were you able to

determine whether or not those registries and registrars that were unwilling to respond to a request without court order, if they also happen to be associated more with bad actors? If that was something that would be useful to gather even if just anecdotally? Figured I would ask the question, thanks.

LAUREEN KAPIN: I am not certain. Does anyone have the answer to that? I don't know the answer to that. I would be - I would speculate that I would be surprised if this particular survey got into that level of detail. That said, it's certainly a worthwhile question to ask. Kavouss, I see you but I also wanted to let someone who hasn't spoken go first. The gentleman who is raising his hand and then I will loop back to you, Kavouss. Go ahead.

EUROPEAN COMMISSION: I would like to thank also the podium for this presentation and also for enlightening the GAC regarding the survey on the impact GDPR has on the - I think every evidence that we get on the issues to help us to prove also EPDP, but also in general in the community, to help us make the case are very, very welcome.

Now I I want to stay a little bit on the presentation about two points. The one was about the necessity of keeping also the historical data which ties up to the question of the retention period, whether we have some clear evidence about what is the required retention period to

serve the purpose of what the activities he referred to are necessary, even if we have an approximation that would be very, very important.

And the second point I would like to ask was whether there was a certain study that was saying that in cases where we have increased accuracy in the WHOIS data, then the malicious activity, which I expect was reversely important. So whether also the question of having accurate data in the WHOIS also helped at preventing cybercrime.

LAUREEN KAPIN: Thank you. It's hard for me to see, which is why I didn't call you by name. Apologies for that. Did you want to take up the retention issues and the importance of WHOIS accuracy information?

GREGORY MOUNIER: On the data retention, it depends on who are you are asking to. If you ask an investigator who has been investigating countless cases for several years, he will tell you that he wants 15 years of data retention. Because you never know. Because he has cases where it could make a breakthrough because there was connections or correlations to data that has been kept longer.

But obviously, this is a question that the legislator or community in this case has to state. If you asked law enforcement, if you asked everyone on this panel because of our job, we will tell you we want the longest data retention period possible. But if you ask somebody who is involved or data protection experts they will tell you the principle laid down in GDPR is that you minimize that retention period to what

is necessary. What is necessary for law enforcement is the longest data retention period. And I'm being very blunt. But our rule is to pass on that message and your role as a community as a legislator is to strike the right balance. But if you ask the law enforcement community, we want the longest data retention periods. I know it's contentious, but I think this is just the choice.

As to the accuracy of the data, having accurate data is essential, but it also means that you have a lot of checks, a lot of KYC measures implemented And that's the most important. Because without those rolling measures, if you don't have the proper process that checks regularly the data, if the contracted parties are not spending resources, and I know it's costly to check the information that the registrants are giving them, then you won't have accurate data.

If you are a serious criminal, you will always be able to register a domain by stealing the identity of somebody else, so technically will be accurate data. It will just be stolen information. So yes, accurate information is essential, but you also have to have all the measures and the processes to keep that information accurate and yes, it helps to attribute crime.

IRANGA KAHANGAMA: And just to follow up on the accuracy point, I think it's a really good point and I think it's something that has been around even before the GDPR. Specifically, as an example, in terms of validating and verifying information and ICANN's contractual requirements, I believe there is a cross-field validation requirement that still hasn't been implemented.

And so this is when you would have a service run a check to make sure that the format of an address would be valid and at least formatted correctly, if not actually the address existing.

So I think this is just one example that was built into the contracts a long time ago that is a nod to the fact that information needs to be more accurate and more valid to be beneficial to the whole community. Thanks.

LAUREEN KAPIN: Other questions? And Kavouss, I know you had your hand up.

KAVOUSS ARASTEH: Yes, during the presentation the distinguished person sitting on your lefthand side mentioned that they want to have immediate access. That doesn't exist. There is access, but the adjective immediate is not there. There is another adjective, reasonable, lawful, legitimate, and so on, so forth. There is no immediate access, unlimited, unconditional access, so we should be taking that into account.

And what is reasonable, still the PDP is discussing, this we don't know. Even the charter mentioned that reasonable [inaudible]. We have to see what is reasonable. Who decides that this is reasonable or it is not? Nevertheless, lawfulness we can discuss, legitimacy we can discuss, but reasonability we don't know. And it's limited also. There are many, many vague things, but there is no immediate access at all. Thank you.

GREGORY MOUNIER: Thank you very much. So let me just specify a little bit what I meant. Immediate access doesn't mean that id doesn't - it has to be lawful, we agree with that. It has to be reasonable. What I meant is, technically what the law enforcement community needs is I need to log into a GDPR compliance system that allows me as an investigator to check straight away whether the information on a domain that I'm investigating right now, what I mean by immediate, is that I don't want to be waiting for nine months to get back information on registrants.

I just want the community to build a system which GDPR compliant, which is lawful, absolutely. But then, you have to understand that we need to have that information straight away. We can't be waiting for a registrar to make an assessment whether this seems to be in line with the temporary specifications and come back to me in one month. Because my investigation is ongoing. I need to get the information right now. And I think this is absolutely compatible with GDPR.

LAUREEN KAPIN: Just to build on what Greg is saying, Kavouss, you are right. The word that's used is reasonable. And you're also right. The issue is, what does reasonable mean? And I think what you're hearing from my colleagues on this panel and what we heard yesterday from our law enforcement and public safety and consumer protection colleagues is that for us, reasonable needs to be very quick because of the pressing needs of these investigations.

KAVOUSS ARASTEH: What Greg mentioned, if I'm correctly referring to his name, is different. Once the access requested reasonable legitimate, this information can be provided within x days. Are you talking that? You want to have the days? When you say immediately, not waiting nine months. How long can you wait, one hour, two hours, one day? So we need to inject that into the process of EPDP. Once this access legitimates [inaudible] the registrar shall provide this information within and then we say. If that's the case, please let us know, we can visit. Thank you.

LAUREEN KAPIN: Thank you. So we're a little over time so we're going to transition into really a continuation of the topic that has kept our attention here and that is GDPR issues. I want to thank everyone for their attention, for their early arrival and continued engagement on these issues. And doesn't need to stop with the conclusion of this formal panel. My colleagues are always available in addition to myself to engage with you one on one and continue this dialogue. Thanks so much for your attention.

[END OF TRANSCRIPTION]