DUBLIN – GAC Public Safety Working Group Open Session
Monday, October 19, 2015 – 15:00 to 16:30 IST
ICANN54 | Dublin, Ireland

ALICE MUNYUA: Good afternoon, everyone. This is such a large room, we'd like to request you to come closer so that we can feel a little bit more intimate. I know we are competing with several other sessions, the CCWG, but this one is a very important one and it would be nice to have you closer, please. Thank you.

Good afternoon, everyone. My name is Alice Munyua. This is a meeting of the Governmental Advisory Committee public safety working group. The public safety working group is a GAC principle 27 working group, and it focuses on those aspects of ICANN's policies and procedures that have implications for public policy. Public safety, rather.

The working group was created in Buenos Aires, terms of reference officially endorsed by the GAC, and the primary members are expected -- or are representatives from law enforcement agencies, from different countries, including consumer protection groups, criminal and law enforcement groups, and other agencies responsible for public safety.

If you're interested in having a look at the terms of reference of this GAC working group, you can go to the GAC Web site. We have a working space for the PSWG where the terms of reference are contained.

We have a rather long agenda, but the first thing we'll do is introduce the panelists.

I will say my name is Alice Munyua, co-chair of the public safety working group from the African Union Commission.

WANAWIT AHKUPUTRA: Wanawit Ahkuputra from Thailand. I'm also the vice chair in the GAC.

LAUREEN KAPIN: I'm Laureen Kapin from the United States Federal Trade Commission focusing on consumer protection.

ROBERT FLAIM: I'm Bobby Flaim, FBI.

JOHN CARR: John Carr, from the British Children's Charities Commission -- Commission -- Coalition on Internet Safety.

CATHERIN BAUER-BULST: Catherin Bauer-Bulst. I'm from the European Commission. I'm the team leader for The Fight Against Cybercrime and Child Sexual Abuse.

GREGORY MOUNIER: Good afternoon. I'm Gregory Mounier. I'm from Europol, the European law enforcement agency, and I work as the outreach team leader for the European Cybercrime Center.

NICK SHOREY: Hello there. My name is Nick Shorey. I am a member of the U.K. GAC team and I work for the Department of Culture, Media and Sport. Thank you.

JON FLAHERTY: Hi there. Jon Flaherty, United Kingdom National Crime Agency, National Cybercrime Unit. Thanks.

ALICE MUNYUA: Thank you very much.

We have a very distinguished group of panelists and we look forward to very vibrant discussions.

We're going to move straight ahead. We have quite a long agenda. We're going to be looking at first an update on what the

public safety working group has been working on since Buenos Aires, and then we'll look at WHOIS and European data protection laws, and then some case examples of WHOIS from Europol and a roadmap on how the public safety working group works at the national level and the capital -- and coordination at that national level, and then spec 11 on the new gTLD security framework, and then a presentation or a discussion on child exploitation and new gTLD strings.

So we're going to go straight to the agenda and I'm going to call upon Laureen Kapin to take us through the updates and public safety working group comments to date.

Laureen, please.

LAUREEN KAPIN: So first of all, welcome everyone. Thank you for joining us in this cavernous room. If anyone wants to move closer, we promise we will not be ferocious and we will welcome that so the room feels a little closer together.

If anyone has trouble hearing, give a wave and we will try to speak more slowly or more loudly or more clearly. And there will be a number of presentations today and we'll have Q&A after each presentation, but of course if you don't get a chance to ask

your question now, please feel free to find us in person and we're always happy to chat with you.

My colleague, Bobby Flaim, is going to be handling this topic with me and we'll be tag-teaming, so with that said, we will launch into it.

So again, this is the public safety working group. We wanted to start off with a little bit of context for you. Although our public safety working group is new, the folks who have been advocating for public safety have been involved with this type of advocacy work for quite some time. Over 10 years. And during that time we've advocated on a number of different issues.

For example, we've advocated to create consumer safeguards for new gTLDs, and that process had a formal expression in the Beijing communique, where a whole set of safeguards applicable to new gTLDs were advised by the GAC and a lot of our recent work has focused on making sure that that advice that was accepted by the board was implemented.

So we've been focused on that for quite some time.

Bobby's going to speak a little bit about some improvements in contract provisions.

ROBERT FLAIM: Yes. One of the things that we had focused on, you know, before the creation of the public safety working group, if you remember the law enforcement recommendations, so that was something that we did over a number of years. 2009 to 2013. And we continue to be involved with that, with some of the specifications and working groups that have arisen out of that, such as the WHOIS specification, the proxy privacy working group, and a few other things.

So obviously that's something that touches upon public safety and domain names.

The other thing that you see on there is the improvement of WHOIS accuracy, and that's kind of where we started. And you're going to hear a little bit about that further from Catherin and Greg later on insofar as how WHOIS accuracy is important to the work that we all do as public safety officials and also get kind of a flavor of what Europe does and how they balance European protection laws and also the public safety concerning WHOIS accuracy.

So just, you know, like we said, we've been doing it for 10 years and as consistent themes that we have continued to be a part of.

LAUREEN KAPIN: So the big takeaway for this first section is even though we're a newly launched working group under the Governmental Advisory Committee, we've actually been active in advocating for quite some time, but now we have a more formal channel of communication for our advocacy work under the umbrella of the GAC.

So recent work.

I want you to know, as Alice indicated at the beginning, that if you're interested in looking at some of our recent work, the GAC Web site is the place where you can find it, and all of the GAC working groups, in fact, have a public space on the GAC Web site. You don't need to be a member of the GAC to access that information. Here's a link to our particular site. And the Web site also includes information about the public safety working group representatives and various comments that we have submitted.

So that's the place if you want to read about it with your own eyes.

So we're going to take you through kind of a short highlights session of some of our recent work.

Bobby, you want to talk about the 2013 RAA, because I know that that's a subject that's near and dear?

ROBERT FLAIM: Yes. As part of the -- when the 2013 RAA was signed and it came out, one of the -- there was a couple of things that came out of it that kind of laid out groundwork for future work, and one of them was the WHOIS specification where that would be reviewed.

So this year during 2015, there was a discussion on how to look at the WHOIS review -- or the WHOIS specification that is part of the RAA and see how it can be improved or changed. So I know ICANN and the registrars had a -- a few issues and comments about it, and there was a public comment period that was opened.

So we, as the public safety working group, actually did contribute to the -- to the public comments.

So we had done that. We had also spoken about the -- or made comments to the privacy proxy working group. And I think the last thing was the next-generation WHOIS that was also opened for public comments.

So one of the great things about the public safety working group is that now as part of the GAC, we're able to focus on these very specific issues, and even though at the beginning we kind of had a disproportionate law enforcement representation, we have

kind of opened it up -- or it was opened to other government officials that deal with public safety, such as Laureen's agency, which is consumer protection, civil law enforcement, and other public safety organizations such as the Food and Drug Administration in the United States and its equivalents worldwide, and other such agencies that have impacts on public safety.

So that's why you're seeing some of these comments that are being drafted on by the public safety working group.

And I guess the first one we have up there -- I'm sorry -- is the WHOIS accuracy, which ICANN, prior to the Buenos Aires meeting, had made comments and the registrars made comments and we actually even had a public session there.

And one of the things that we were interested in is to try to get some more specificity in some of the comments that had come out.

Namely, some of the time periods that were discussed by the registrars and also some of the qualifying language such as "substantial" and "substantiate."

So we were just trying to get a little more definition on that and how that would work with the WHOIS specification, because as

you're going to hear a little bit later on, that is something that we use and it is something that we have interest in.

LAUREEN KAPIN: And for a little more context here, the 2013 RAA does have some obligations about registrars having to verify the accuracy of that information and a time period to act if they don't get the verification, if there's complaints, et cetera. And some of the questions we have really focused on the wisdom of lengthening this time period for response, especially if there is no response back from the person who is supposed to provide accurate contact information.

Another area that we have submitted a comment on is privacy proxy services, and this was in response to the privacy proxy working group's report on that issue.

And this -- this service essentially allows entities to mask their information and there can be reasons for doing so, and there also can be concerns that are raised when that happens.

So the public safety working group submitted a comment on some of the issues in that report, and we drew a line where we thought that there should be a distinction made in terms of the availability of those services. And more specifically, if there's a context where commercial services are being offered, i.e., where

you as a consumer are being asked to provide your financial information -- a bank account, a credit card number, et cetera -- that you really have a right to know who you're dealing with. And consequently, privacy proxy services shouldn't be available in that sort of situation.

We also emphasize that there should be transparency and accountability for privacy proxy service providers, and that when law enforcement makes a request for information about who's behind a domain that may be the subject of investigation, that those requests should be kept confidential as it's required or permitted by local law, because often law enforcement has an interest in keeping the fact of its investigation confidential so that evidence and assets don't disappear.

And then we also --

Right. That's the wrong device. That shut off my microphone.

We also submitted comments on next-generation WHOIS services which Catherin is going to be talking more about. That's a really complicated issue really focusing on what's working and not working now with WHOIS, whether there should be a subsequent system, and if so, a whole host of questions about what that system should look like, who should have access to information, and really what we emphasized in our comment to this preliminary report is that, one, it's

complicated, and two, there really needs to be a balance struck respecting consumer rights and keeping the public safe and also securing the protection of personal data of Internet users.

So really are advocating for balancing those viewpoints and keeping communications open because these interests are not irreconcilable.

Indeed, the Federal Trade Commission in the United States deals with both consumer protection and privacy issues all under the same roof. We're all friends, we discuss issues with each other, and there's balances to be struck.

So that's one of our takeaways and that will continue to be an area that's very important to us.

ROBERT FLAIM: So one of the other things that you're going to hear from, from Jon Flaherty from the National Crime Agency, is the Specification 11, which is the registry agreement security framework, and that's something that originated through GAC advice in Beijing, so about two and a half years ago.

So we've been working with that, and John has been representing the public safety working group in working with the registries to come up with voluntary practices to kind of flesh out how that would work insofar as dealing with abuse such as

botnets, phishing, child exploitation, so on and so forth, so we have a cooperative agreement with the registries on how we can effectively deal with that abuse and with criminality. So you're going to hear about his work later on today, but just to flag that for now. That's another thing that the public safety working group has worked on as well.

LAUREEN KAPIN: And future work. What's -- what does our crystal ball look like.

Well, we're hoping to have representation on the upcoming working group on competition, consumer choice, and consumer trust. That's going to be a very crucial working group to take a hard look at all those very important issues.

Besides WHOIS accuracy for domain information, there's also...

ROBERT FLAIM: Yes. One of the other things that's very important in how we, as public safety officials, in looking for attribution or in looking for abuse, is also the other side of the coin. Not just the domain name system or DNS, but also the IP addressing system, which is managed by the regional Internet registries.

And here they are the addressing supporting organization. Outside of ICANN, they are the numbering resource

organization. So we're trying to work with them to kind of match up some of the things that we've done here at ICANN with the registrar accreditation agreement, some of the IP accuracy requests, so that they would be able to do the same thing.

Now, as regional Internet registries, there's five of them, so we're trying to work with them to come up with global policies, coordinated global policies with them, so they would have kind of the same voluntary practices to ensure WHOIS due diligence and accuracy as well.

LAUREEN KAPIN: And finally, it is our hope to have more participation from the public safety working group and existing ICANN working groups. We also want to focus on outreach to our other government partners. All of the countries up here and in our group have a lot of different agencies with individuals with tremendous expertise on keeping the public safe in a variety of contexts, and those are people who can be important allies and sources of guidance for our group.

And of course our other stakeholders at ICANN also have a wealth of information and perspectives that we find valuable, so we'll also be focusing on outreach to get the wisdom and guidance from our partners in the ICANN community.

So that's a little bit of a snapshot, a highlights reel of the type of work we've been involved in and what we hope to focus on in the future.

On those issues, if folks have questions, this would be a fine time to use the microphones that are set up to ask them.

There will be other presentations as well, but we thought it would be more orderly to take a few questions after each presentation.

ALICE MUNYUA: Thank you, Bobby and Laureen. If there are any comments or questions, we've got two microphones at the front of the room here. Please come forward. Thank you.

Please, your name and -- yeah.

VOLKER GREIMANN: Volker Greimann, GNSO Councillor for the Registrar Stakeholder Group. We have been working as registrars with WHOIS accuracy for as long as we exist, and I think it's an important issue. However, there's also the counterpoint WHOIS accuracy which is privacy concerns. So I would like to see this working group with the background to also tackle the implications of WHOIS accuracy to the privacy of the users of the domain names

to advise ICANN on how to best protect the privacy -- the private data of the registrants, i.e., is a public WHOIS really what you need or if a different system, a non-public system or half public system would be something that's better suited to your needs as well?

ROBERT FLAIM: I think you are going to have a lot of those questions answered when Catherin gets to the microphone. She's going to talk about the European data protection and maybe some of the issues or challenges with the next generation and how we balance those things and what might work and what might not work. So I don't want to steal your thunder, but I think that's what we're going towards and may answer your question and address some of the concerns.

UNKNOWN SPEAKER: Perfect. Thank you.

UNKNOWN SPEAKER: Good afternoon. My name is Arthur Zonnenberg. I work for Hostnet, a Dutch registrar, ICANN accredited. Besides the point I share with Volker about European issue, like why would the Federal Trade Commission of the United States determine or influence my privacy as a European user. I would like to know a

little bit more about the rationale you talked about that if somebody gives you their credit information or gives you payment information, that that would entitle them to know who you are and know who they are dealing with in the case of a Web shop, of course, would be logical to get service. In the case of, for example, an activist working against certain vested interests, which is why they want to remain private. But at the same time, I want to support their private calls and their anonymous calls, if you will, to be able to support people that go against vested interests of major corporations and, of course, the U.S. has always been criticized, perhaps unfairly about being in league or playing too much to these interests. So I would like to know a little bit more about this rationale that as soon as I give you my credit card information that that would entitle me to your personal details.

LAUREEN KAPIN: First, let me say there are differences of opinion on this issue. And from the consumer protection standpoint, if someone is providing that sensitive information, then our perspective is what you perfectly, of course, to disagree with, that we are entitled to know who we are dealing with. And I fully understand the sensitivities about advocacy groups.

Advocacy groups can choose to take financial information or just advocate their views. But if they take that step and they are dealing with that sensitive information, then it's our perspective that the public, that the consumers have a right to know who they're dealing with. And that's one perspective. We realize that not everyone shares that perspective.

ALICE MUNYUA: Please go ahead.

UNKNOWN SPEAKER: Thank you very much. Mine is not a question but rather a comment. As much as this is drived out of GAC, I would encourage that there are more members because you have law enforcements within different countries that have totally not been involved in this procedure. So I would request that we have more involvement from that perspective.

My name is Gloria from Uganda.

LAUREEN KAPIN: Thank you.

ALICE MUNYUA: Lee.

LEE HIBBARD: Hello. My name is Lee Hibbard. I'm from the Council of Europe in Strasbourg, in France. We're an intergovernmental organization of 47 countries dealing with many things including cybercrime. We have the Convention of Cybercrime, the Budapest Convention. And we also deal with data protection issues -- and I will pass to my colleague in a second -- but also Internet pharmacy issues and online drugs and the quality of health and medicines and healthcare online.

It's really a point just to say about outreach. I want to put the Council of Europe on the map here in the public safety working group. We are an observer to the GAC. We are member of this group now. And we would really like to bring the expertise from the different work of the Council of Europe into this group.

You talk about outreach. We already have a lot of expertise to share with you. We already sent comments to the mailing list already.

Just to complete and to pass to my colleague Peter, we have -- the 47 countries in June this year agreed on a new declaration on ICANN, human rights, and the rule of law. And that really means to put on the map the questions of human rights and making sure that ICANN respects through its policies and

procedures on human rights and rule of law issues. We are really here to bring back expertise into this group.

And I will pass to my colleague, Peter. Thank you.

PETER KIMPIAN: Yes. Good afternoon. My name is Peter Kimpian. And I'm representing the T-PD of the Council of Europe, which is an advisory body of Convention 108. And I'm really happy to be here. This is the first time.

And I join my colleague Lee on suggesting you cooperation and giving you our expertise as much as we can on data protection and privacy issues.

I think the right word as our colleague from the U.S. rightly pointed out is balance and there are no unreconcilable issues.

The best thing -- and I'm saying that as an officer of data protection authority in the European Union -- is to sit down at the same table and openly debate questions and to find the best possible solutions. So we are very open to that and very happy to be here and offering our expertise, our work, and energy. Thank you very much.

ALICE MUNYUA: Thank you, Council of Europe. And we do have a closed meeting later that you are aware of and you are members of the GAC. So, yeah, you're welcome.

David.

DAVID CAKE: Thank you. David Cake from Electronic Frontiers Australia and NCSG. I have got two comments, one sort of specific and one more general.

The specific comment was to say we did receive your input in the PPSAI working group. And our decision is going to come out -- you know, in the opposite way to what you recommended, I'm pretty sure. Please be aware -- we certainly did consider it, but it came in after we had already debated those issues in quite some depth. And we had something like 60,000 responses from the general public. And, you know, you came in quite late as well. You may need to try a bit harder -- get more involved in some -- when it's particularly a contentious issue.

I think -- I understand that you are a new group and have come -- but, yeah, just wanted to let you know that more engagement may be necessary in some of these things.

Another one is a general sort of comment. Data protection agencies -- I mean, data protection laws are laws and they are

about public safety. Data protection agencies are law enforcement agencies and public safety agencies, but they are sort of notably absent from you group.

To really be seen as a strong voice, it would be good to be inclusive so you feel like we're reflecting a broad law enforcement rather than part of it. If it's sort of a part of law enforcement, then you are another lobby group rather than a sort of -- be seen as representing all law enforcement and public safety agency views. So I would encourage you to be more actively inclusive, particularly of data protection agencies, in your comments if you want to be seen as a strong unified voice for public safety in law enforcement.

ALICE MUNYUA: Thank you very much, David. I can assure you we are not a lobby group.

[Laughter]

DAVID CAKE: I know, I understand. All I'm saying is you need to make sure you are inclusive of those particular voices within the law enforcement community because, otherwise, we will be seeking out those voices and worrying about how the dialogue is happening.

ALICE MUNYUA: We take those comments very seriously, and we did have that discussion yesterday when we the discussions with the GNSO. You were present.

And one of the issues that came up is that the GAC does need to get involved a bit more earlier in some of the processes, especially the PDP processes. And to that end, we've already started working towards that.

But there is also trying to understand governments generally work. We do need to consult at capitals. And we actually do need to consult with different -- various stakeholders. So my apologies if sometimes comments come in late. But we are going to be trying to ensure that we are working very closely with the processes. And to that end, we have members who are going to be joining some of the working groups. We are contributing directly as a GAC working group. Thank you for those comments.

DAVID CAKE: I understand that you are a relatively new group and that you have not -- some of these working groups currently predate you. So, of course, you can't get in an early stage without a time machine.

But the -- I would commend to you all the work that's being done in the GAC-GNSO coordination group about how to get the GAC involved earlier in GNSO PDPs. The GNSO really does want your input. And the earlier we get it, the better for everybody, particularly GAC input and particularly from -- particularly GAC input if it comes in quickly after the -- ideally even after the initial report. That will really help shape the direction the working group goes. It's easier for everybody if you help shape it early on rather than try and respond to our conclusions which is not, you know, necessarily -- which is often a very difficult position to argue from after we have already made a decision more or less.

ALICE MUNYUA: Thank you, David.

Do you want to respond?

Okay.

AMADOU LY: Hello. I am Amadou Ly. I am a member of the telecommunications regulatory agency in the Republic of Senegal. I commend all these working group members for the work you've done. And I have several questions regarding safety information or data protection, especially in countries like mine,

African countries like Senegal, where to date, we have people working in governmental agencies, in public administration who still use generic email addresses such as Yahoo!, Gmail. And we do not have enough Internet connectivity to have a .GOV domain extension.

We do have members of the government that use email addresses that date their times in college. This is a fundamental issue. Internet today has reached unheard-of levels. People handle confidential data in public administration, departments. And they don't realize that they're handling that data by using a Yahoo! or a Gmail account. Can we protect these people without stopping our work with databases? People that handle important, sensitive databases do not realize that they are handling highly important and crucial data for governments. And this information is hosted elsewhere. And we do not have message handling or management policies, et cetera.

This is even more noticeable when we read people's business cards, and we see that they use a Hotmail or a Yahoo! email account.

So, we do need to know who we work with and who you work with. We need to work with these people that are handling sensitive data and who do not have the necessary resources or levels. So you have to see on the way you can work or what you

can do to ensure safety and data protection. We can have firewalls, et cetera. But if we're not -- or if we do not feel safe when we engage in a transaction and we don't know what happens with our data, then we face a big issue that calls for a lot of common reflection, thought, and work in a collaborative fashion with all stakeholders so that data is protected.

Thank you.

LAUREEN KAPIN: Well, I think you raise a lot of very important issues. And certainly there's a lot of education that I think needs to happen for the public to know how to be safe on the Internet and how to view emails from a Gmail and a Yahoo! account, even if someone says they're from the government.

I'm not going to be able to answer all the questions you raised because they're such big, complicated questions. But I do know that there is a real need for educating the public to be very cautious when they are using the Internet, whether they're buying something, whether they're on a dating site, whether they're getting emails that say they've won a contest, or from someone who's pretending to be in love with them and in need of some cash because an emergency has happened. Those are all very important issues. And I think it's something that we all need to be aware of and be working on because people's lives

can really be harmed in very bad ways by people seeking to take advantage of them when they're on the Internet.

ALICE MUNYUA: Do you have another comment or question?

AMADOU LY: Thank you for this question. The question that I ask myself is the following. In ICANN, we work also with large companies managing databases such as Google. So what should we do with them? What can we do in a general manner in order to make sure that the databases are managed in safe manners?

I agree that the managers are responsible for their actions, but I believe that there should also be a responsibility on all the database managing companies that also host all the transactions. I agree with you that we have to be on the alert.

I would like to know which of the actions or the steps that we could implement in order to make sure that we have secure transactions. That was the aim of my question.

ALICE MUNYUA: -- to the next session, Catherin from the European Commission is going to speaking about exactly some of those questions and issues you've raised and raised by another speaker.

She's going to be talking about WHOIS and European data protection laws which might give us several examples on how we can address the same issues in some of the African countries or other countries for that matter.

Thank you. Catherin, please.

CATHERIN BAUER-BULST: Thank you, Alice.

I don't know whether I can provide solutions for the whole world, but I'm very glad to see the strong interest in this topic. And as Laureen already said, there's -- and as many of you have raised, there's a balance to be struck. And in my experience, these types of debates have always benefited from a solid evidence base.

So what I want to try today is just to sort of do a very brief introduction on the E.U. norms governing data protection and on the implications that those norms have for processes such as the thoughts about redesigning the WHOIS.

When I was preparing for this, I looked back at the long history that the WHOIS discussion has already had and at accountability in general. And I realized that the history of the discussion on accountability and whether or not we need accountability actually goes back a long way farther. In fact, I found it first

mentioned in Plato's Republic 2,000 years ago where, as some of you may know, there's the story of a Ring of Gyges, which is the story of a shepherd who tending to his flock was wandering around the hillside and stumbled upon a cave where he found a ring that, lo and behold, when he put it on made him invisible.

Now, emboldened by this invisibility, he went to the court, slayed the king, laid with the queen, and took over the government. And this parable is told in Plato's Republic at the basis of a discussion around accountability where the somewhat sour conclusion that Plato and his friends drew is that accountability in a sense is a moral construct. And as soon as you take away the ability of others to see you, there's no very strong incentive any longer to act morally.

So apparently these problems, we're not the first facing them. And I don't know whether we will be coming up with the perfect solution.

But why I don't necessarily think it has to be seen as a tradeoff, per se. In my work as cybercrime, in fact, I see myself as being on the front lines of data protection because I try and to prevent data from being stolen. Identity theft, the theft of payment credentials, the trade in child sexual abuse images -- all of these are gross violations of privacy. And we're working very hard to

enable law enforcement to be able to prevent and protect and prosecute people for those crimes.

So what are the -- I want to sort of represent the views of both sides here. So let me just briefly recap what the law enforcement concerns are with the WHOIS.

In ICANN's Affirmation of Commitments, they have undertaken the obligation to maintain timely, unrestricted, and public access to accurate and complete WHOIS information. And to review the effectiveness of the WHOIS policy every three years.

And the Governmental Advisory Committee in its 2007 communique additionally established a few principles of what the WHOIS should do; namely, to assist law enforcement in investigations and in their possibilities to enforce national, international laws; to assist in combating against abuse of uses; and to assist businesses and others in combating fraud and safeguarding the interests of the public.

Now to go back to the fundamentals, now, from a European perspective, data protection and security are both fundamental rights. They're enshrined in the EU charter of fundamental rights in Articles 6, 7, and 8, which, basically, say that everyone has the right to freedom and security and everyone has the right to respect for his or her private and family life, home, and communications.

Now, the EU charter is a modern charter in the sense that it already contains rights relevant to digital society such as guarantees in bioethics and transparent administration, but also something more specific on data protection. So in it's Article 8 it does say that everyone has the right to protection of personal data concerning him or her.

It says that data must be processed fairly and that everyone has the right to access data which has been collected about him or her and to make sure that that data is accurate. Now, these are key rights in a democratic society, and they are not absolute. So each of those -- the rights to security and the rights to privacy and data protection have to be balanced with each other and with other fundamental rights.

Now, I just want to briefly highlight the key provisions of our main legal text, which is a directive on data protection on the protection of individuals with regard to the processing of personal data.

What we've heard -- we've heard a lot of concerns in the past about the fact that there isn't a unified voice from Europe basically outlining the concerns and outlining the data protection requirements. And a lot of that is due to the fact that the legislative instrument at the basis of this is a directive, which is a special type of legislative instrument that is binding as to its

goals. But it leaves it to the 28 EU member states how they want to implement their own national legislation in order to reach those goals. And that means that we do not have one set of identical laws, but rather we have 28 sets of laws that strive for the same aim but that do not necessarily contain the exact same language.

So that is a challenge.

But, in fact, we are currently working on adopting a new package, a new legislation on data protection which, hopefully, should be passed even by the end of this year. And that will be in the form of regulation. So there we will actually have a law that no longer needs to be implemented in different ways by the 28 member states but that applies in and of itself right away. So, in a sense, you might be getting more consistent answers from the European countries on some of these issues after this has been implemented.

So I just want to explain briefly the definition of personal data that we use in the EU.

It, basically, means any information relating to an identified or identifiable natural person.

You will note it says nothing about the sensitivity of that information.

So, really, the only -- the only key factor here is whether or not you're able to identify a person. So a name, obviously, is personal data. An IP address can be personal data. It can also be -- if you say, to take an EU example, a multi citizen working for the European Commission in DG XY and Z, that can also be personal information because it is something that allows somebody to identify that person.

Again, there is no -- doesn't matter whether the information is sensitive. So the concept of personal data does not differentiate, e.g., between content or traffic data or subscriber information. It can all be personal data.

The other key concept we have is that of processing. Basically, I have a colleague who refers to this as the Midas touch. Anything you do with data is processing. Whether you look at it, you store it, you delete it, you move it, you disclose it, everything is processing.

So what are the requirements regarding processing? First of all, you have to have a reason. You have to collect it for specific purposes. You need to make sure that the amount of data is relevant and not excessive in relation to those purposes.

The information has to be accurate and kept up to date. It may be kept no longer than necessary. And the whole exercise needs to be legitimized by a justifying ground. That can be the consent

of the data subject or the fact that you need the data for the performance of a contract or a few other reasons.

Who are the main actors on data protection? I was just talking about the adoption of the regulation. That will be adopted by the Council of the EU and the European Parliament, which are our legislative actors.

I'm from the European Commission which is in charge of proposing legislation and of monitoring its implementation.

Then we have the national data protection authorities which will be in charge of monitoring the implementation of data protection at the national level. And the article 29 working party, which some of you will be familiar with because they have occasionally submitted comments to various policy processes. They are, basically, a working group that brings together the national data protection authorities and commission in an advisory capacity. So they, basically, give advice to the Commission and to others on how data protection laws are implemented.

And, finally, we have the Court of Justice, which is the only institution that is authorized to interpret data protection law. So they're the ones who give us the straight answers on how to interpret the data protection regulation.

Now, what does this mean for the WHOIS? If we're redesigning the WHOIS, there's three central aspects that we're going to be looking at both from a law enforcement and from the data protection perspective. The first one is availability. So here, as we learned just now, the data has to be collected for a legitimate purpose subject to a legitimizing ground. So it has to be collect with the consent of the data subject, for example. And any future registry directory service should ensure that the purpose is made clear; namely, that this is also for accountability purposes to make it clear to the data subject that this is also for their -- for the eventual access of law enforcement agencies. We should collect no more data than is necessary for that purpose, and we should keep it no longer than is necessary.

Now, access -- the fact that this is currently a public system and also that ICANN has committed in its Affirmation of Commitments to keep it public, that's going to be a key issue to be looked at. From a data protection perspective, the directive does not say anything about limiting access to data. But, obviously, from the spirit of the law, it would be helpful if the data was not disclosed unnecessarily.

And for the accuracy parts it's actually quite easy. Because here data protection law enforcement are exactly on the same line. We both -- both perspectives ask for accurate data.

And that's it for me. I'd be very happy to take any questions. Thank you.

ALICE MUNYUA: Thank you very much, Cathrin. If there are any questions or comments, please come to the microphone.

Maybe then we can hold any questions or comments and move on to the next session. That's looking at case examples of WHOIS presented by Greg from the European Cybercrime Centre.

GREGORY MOUNIER: Hi, everyone. Can you put the slides on maybe?

ALICE MUNYUA: Oh, you have a question. Please introduce yourself.

VOLKER GREIMANN: Hello. Volker Greimann, GNSO councillor for the registry stakeholder group.

Thank you for your concise and very interesting presentation on the European position on data privacy.

I think what has been clear and has been clear for a lot of us, many of us from the beginning is WHOIS, as it stands now from

the private data of millions of citizens, is published every day for anyone to look at is problematic under the European -- from the European data protection standpoint and maybe even the data protection standpoint of other countries as well. This would necessitate a clean cut or revision of WHOIS as it stands today and in such a way that the data is not freely available any more. Would you agree to that and what would you think, from the public safety working group's perspective, how such a regime should look like.

CATHRIN BAUER-BULST: I think I agree with you that, from an ideal perspective, there should be -- there should not be open access to all data that's currently available. The question is how to balance that in practice with the needs that WHOIS is there to fulfill. And there is also in the EU legislation, in fact, requiring information to be published on Web sites, for example, for every actor who is not acting in a strictly personal capacity. So, if you're not just posting your family pictures for your friends, then you, in fact, not only have to comply with the WHOIS obligation. But you also have to give on your Web site detailed contact information to be held accountable if anything illegal goes on with your Web site.

So, in a sense, also within the EU, this balance has to be struck. And it can go either way in many circumstances. I'm not sure what the perfect system will be for the WHOIS. I don't think anybody is at this point. And where -- we're just trying to, basically, look at the concerns from both sides and trying to reconcile them here. But I'm afraid I don't have the perfect solution yet.

VOLKER GREIMANN: That's perfectly fine. We could work on WHOIS for years and not find a solution.

[Speaker off microphone]

Just as a follow-on, I would like to make sure that, when you deliberate this topic, that you differentiate between content which Web site presences are aware a certain amount of openness about who is publishing certain information is beneficial. And even there it goes -- doesn't go into the private addresses. For example, for private individuals that just have presences and registrations of domain names which may be used just for email for very private purposes that have no publication to the outside world at their heart but yet they're still forcing the registrants to publish their private details.

Maybe you would also want to look at how certain European registries are publishing WHOIS. Look at what Nominet is doing. Look at what other registries in the European space are doing where the amount of data that is visible to the public eye is very, very limited, maybe even limited to the name and the email address. And sometimes not even the email address is published.

So have a look at that and see if that would also form a model, in your opinion, for what the private data presentation to the world in the ICANN context for generic TLDs. Thank you.

ALICE MUNYUA: Thank you. Please introduce yourself for the record. Yes, David.

DAVID CAKE: Hi. David Cake, Electronic Frontiers Australia and GNSO Council. To, again, sort of a general and a specific thing. In general, like I just said, that was a great presentation. Thank you. I think it really does highlight that we need to think about which bits of the WHOIS, you know, principles that we need to adhere to in the long term and which bits are, you know, transient requirements that may change. I mean, I found out only this week that Web sites had been taken down because they don't have the -- I'm sorry -- domain names, registrations are being

taken down because they don't have the required fax number, which is -- obviously, highlights that some things do need to be -- do need to be flexible. But, yeah, I think balancing between the things that will change.

And speaking of things that are changing, specifically, we have the RDDS, Registry Data Directory Services, PDP coming up in the GNSO next year. Well, soon, rather.

That's going to be a huge effort. It will address a lot of these questions about who gets to access what data, what data we collect, who sees it.

I would really like to say that someone -- while, of course, participation via just responding to public comments and all of that sort of thing is very welcome, it would be very, very helpful if we had someone, you know, from article 29 or similar with extensive -- you know, detailed knowledge of data protection who was able to be involved in that process somehow. We appreciate general guidance, but we will have a lot of really specific questions as well.

And I'm warning you now, because I know finding people to take on large tasks like that process is likely to be -- is often not easy. So -- but, as someone from the GNSO's potentially involved, we really in ICANN need people with detailed privacy, deep expertise, and article 29 and so on are likely sources of it. And

we really not just welcome but ask for your involvement. It would be very helpful to all of us.

ALICE MUNYUA: Thank you, David. That's the reason why the GAC developed this working group. And we're certainly going to make sure that we're involved quite specifically in some of these processes and at the earliest stages, as you say. Thank you.

Please introduce yourself.

KIRAN MALANCHARUVIL: Kiran Malancharuvil from MarkMonitor. In response to the lady's comments to Volker Greimann from the registrar stakeholder group, I'm a little bit confused because it seems like what she's saying is directly contrary to the positions that you've taken and some of the public comments that you've recently submitted specifically to the privacy and proxy services accreditation issues group and I think also the WHOIS accuracy specification encouraging open access to WHOIS information and those data fields. So I guess I would appreciate maybe an explanation or a clarification where her statement is somewhat contradictory to the statements that you've submitted officially to those groups.

CATHRIN BAUER-BULST: Sorry. Are you referring to me?

KIRAN MALANCHARUVIL: Yes.

CATHRIN BAUER-BULST: Okay. Sorry. I wasn't quite clear. I'm not sure where I was contradictory. But what I was trying to present are the two different perspectives on this, which is, on the one hand, the ideal situation from a data protection perspective. And, on the other hand, the ideal situation from a law enforcement perspective.

Now, as I was saying in the beginning, these are -- both the right to security and the right to privacy are fundamental rights from the viewpoint of the European Union. And I think that is shared by a number of other regions around the world. And neither of them is granted in an absolute fashion.

So what you have to do in practice is try and strike a balance between them. And that's what we're going to have to do in this policy development process.

And thanks again for inviting us and the article 29 working group representatives to be part of the policy development process. I am going to take that back to Brussels. And I'm sure you're also

in contact with them. But I'll raise it with my colleagues from the data protection unit again to make sure that they know that we would like them on board, that you would like them on board. And then in that process I'm hoping that the adequate balance can be found between these two fundamental rights, neither of which is above the other.

So where they conflict in practice the solution has to be found

KIRAN MALANCHARUVIL: Sure. I think that it will probably be helpful in your further participation within the working group and maybe in further participation in the drafting of these public comments that come through the public safety working group and then through the GAC out into the community if we can have a better example of your opinion on how to balance these things.

Because what we've seen so far is a call for open -- you know, open WHOIS information. And, while we understand that that is -- obviously, needs to be appropriately balanced with legitimate interests and privacy in these regards, it's probably not super helpful to be making absolute statements about the openness of WHOIS. And I think that that's what I was confused about in your statement and sought clarification for. And I thank you for doing that.

CATHRIN BAUER-BULST: No, I fully understand. And it reflects the current policy as it is. So, from a law enforcement perspective, as long as the concerns around a possible tiered access are not addressed, it would be very difficult to have anything else at current. So that's what we're going to have to be looking at in the policy development process.

ALICE MUNYUA: Thank you.

Greg, please. You can -- yeah.

GREGORY MOUNIER: Thank you very much. And I'm going to give you a few examples of where the WHOIS is useful for cyber investigators. I'm going to represent the law enforcement perspective.

Just a few words about the organization I'm working for. Europol is the European law enforcement agency. We are providing support, suppressional support, analytical support to the 28 member states and the police and law enforcement agencies.

On cybercrime, we have established, in 2013, the European Cybercrime Center. We do not have executive power. We rely on

information that is given to us on cases by the member states and our partners. On cybercrime, for instance, we work very closely with the U.K. NCA, we work very closely with the Americans, the FBI, IAS, et cetera. On cybercrime, we have mainly three operational teams. The first one is the focal point Terminal, who is dealing with on-line fraud, payment card fraud, et cetera.

Then we have a focal point called Twins, dealing with child sexual exploitation on-line.

And then lastly, we have the focal point Cyborg which focuses on cyber attacks affecting critical infrastructure and information system, so that goes from the very basic DDOS attack to much more elaborated banking malware and botnets.

Just to set the scene, so I was asked to come up with a few examples that really give you an idea of how the WHOIS can be useful for cyber investigators.

There are many factors that comes into play when you are trying to solve a cybercrime case, but at the end of the day, I think it really often boils down to attribution. We all know that on line, there are many products and services that are very easily available to hide your trace on line and to hide your identity.

Well, there are many examples. I'm not going to list them all. But the point is, in that context, the role of the WHOIS is sometimes critical. WHOIS is one tool, amongst many other others, that the cyber investigators have to overcome the problem of crime attribution.

To be honest, most of the top cyber criminals will not fall because they have the right -- because of the WHOIS, really. They will always use the most advanced anonymity methods to hide their traces. But at least if we have a reliable WHOIS that is accurate with verified and validated user data, then we can drastically reduce the scope of the possibilities for criminals to hide their activities.

So we need to raise the bar, and I think the WHOIS contributes that for the criminals and it really pushes them to resort to more complex techniques to hide their trace, and that's useful.

The first case I want to present to you briefly is a case of a botnet.

So I guess you're all more or less familiar with a botnet so I'm just going to say a few words about it.

A botnet is a network of compromised computers infected by malware that allows a criminal to control that network of computers and to issues commands that are -- to computers

and orchestrate various criminal activities. And what we -- what the law enforcement is after, of course, is the command and control servers that allows the criminal to speak with its botnet.

In terms of botnets and DNS abuse, I think that the abuse -- if you're a criminal and you've really mastered the DNS techniques, and if you manage to maintain a stream of new domain registrations that keeps the botnet fed, then you really have a very robust and profitable botnet.

If you manage again to get new domain names from registrars around the world at a very fast pace, not only you can sustain takedown requests, but you can also sustain sinkholing attempts and of course hijacking attempts from competitors that are also running very powerful botnets, and if they see that your botnet is also very useful, then they will probably want to hijack it, so the DNS technique is very useful for running good botnets.

When I was asked to come up with this scenario, I went to the teams of proper investigators because I'm just a policy advisor, and I sat with them and we went through a series of cases and they looked at it from the DNS and the WHOIS angle, and there was one case, it's a very recent operation, where the Cyborg team was targeting an organized crime group which was

responsible for controlling a botnet deploying on-line banking malware.

They were monitoring the group, and then in a private communication between one of the suspects and his accomplice, they shared details on the domain in question. So what they did is they did a simple WHOIS lookup on that domain and that brought an email address that had been used for registering the domain. They then did a reverse WHOIS lookup on the email address and that yielded a number of other domains that had also been registered using this same email address.

So on those domain names -- among those domain names, sorry, there was one domain which had been created by the individual in question a number of years ago and he had used that domain to set up a personal profile -- professional profile with CVs and photographs. Obviously, that was before his career as a cyber criminal.

So when we used that personal details, we cross-checked it against the national database of the countries in which that person was living and we found out that that was his real identity.

So of course further investigation and sometime later, we proved that that person was, indeed, an active cyber criminal and that led to a successful arrest and conviction.

So the main takeaway of that example is that if you have WHOIS data that is accurate, then you can attribute crime much faster than if you don't. And I want to now give you another example, also in the case of a botnet, distributing webinjects, and that's a negative example, in fact.

So one of my colleagues actually spent three months recently on an operational analysis report surrounding the activities of also a cyber criminal who was developing webinjects to target eBanking customers of banks all over Europe.

So basically what he was doing is that was once the victim who had been infected by the malware would log onto its eBanking portal, then they would unknowingly be redirected to one of the domains registered by the criminal and this domain would present the victim with a Web site very identical to the portal that the person was used to dealing with. And then when the victim would enter his banking credentials, they would be harvested by the criminals and used for fraudulent transfers from the victim's account.

So what my colleague found is that during -- over the last three months, the person -- the suspect had registered 18 different

domains, all for webinjects and targeting customers in Germany, in the Netherlands, and in the U.K. And the suspect had used four different sets of identifiers to register these domains. Names, email address, and phone numbers.

So he did the same technique, WHOIS -- a reverse WHOIS and intelligent -- open source intelligence work on every single identifier, and these resulted to many other identifiers, none of which could lead to any real identity.

The point is that if you -- if you have a criminal that does his job properly -- between brackets -- then you spend very useful investigative time chasing ghosts. My colleague spent three months on that case and he could not find the identity of the guy because the identifiers had been bots off the dot net. They were not legit. They were from identity theft activities. And so you can think that if the registrar at the time had took the pain to validate those identifiers, then maybe my colleague would not have wasted that much time and he could have spent his various full-time investigating other cases.

So that's just an example to show that when you don't have the accurate data, then we lost -- we lose a lot of time.

I'm looking at the watch, so I will not speak about this one. This is also a very famous botnet that we took down, together with the Brits, in February.

Same story. We wasted a lot of time because the WHOIS information was not accurate on the person we were chasing.

But I want to finish up with a positive case. It's a child sexual exploitation case.

These are Web sites that are run by organized criminals, criminal groups. They are not on the dark Web, they're on the open Web, so you can go on that Web site. And what they do is that they sell child abuse material on line.

So basically how it works is that for a monthly fee of about $99 per month, clients can have access, unlimited access, to child abuse material.

So what my colleague did was they looked on those Web sites and they gather the domain names of those Web sites using open source monitoring and some other techniques.

Then they gather the DNS information linked to those domain names -- basically the IP associated to those domain names -- using tools that are available to the registrars and to any investigators such as DomainTools API and so on, and then they gather a CERT set of data from the WHOIS associated to this identified domain.

So in theory, what you get is Domain A has specific DNS information which is -- which indicates that that domain is linked to the IP "A."

Then Domain B, DNS information indicate that Domain B is registered to IP "B." And it -- and so on.

But there's no link between the various domains.

But when you start cross-checking the three sets of data -- the domain names, the DNS information, and the WHOIS data -- then they often manage to find one valid email address that is common to all those domains.

This email is actually used by the registrants to register the different domains, and they need to use one valid email address to communicate with the registrars for billing purposes, for instance.

And so the conclusion of that case was that they managed to arrest a group of criminals and to take down those Web sites. Unfortunately, the business is so good that it -- they keep on popping up.

So as a conclusion, again I will restate a little bit what I've said.

I think that accurate and reliable WHOIS data is extremely important for the law enforcement community to address

cybercrime. It helps crime attribution but it's not the silver bullet. If you are a very good cyber criminal, you won't fail because of WHOIS data. But at least it saves precious investigation time, and I think -- and that's the -- for me, that's the most important. It really raises the bar for the criminals. It makes their life more difficult. And I think that's what the law enforcement is after.

Thank you very much.

ALICE MUNYUA: Thank you very much, Greg.

We have remote participants and we have one question. Olof, GAC secretariat, can read it out for us for the panelists. Thank you.

OLOF NORDLING: Thank you. Yes. This is Olof Nordling, ICANN staff supporting the GAC, for the record, and we have a question from a remote participant by the name of Michael Illishebo. He is an ICANN 52 fellow and working for the Zambia Police Service.

And I quote: "WHOIS is a powerful tool for cyber investigation. However, there are flaws on the part of the registrants. They do not normally give accurate names and addresses during

registration of a Web site, and thus it proves a difficult task during investigation. Is there any way that the registrants will ensure that only true details" --

My screen went black. Oh, it's back again, so I will repeat the last sentence.

"Is there any way that registrants will ensure that only true details are accepted during the registration process? Also, how far has Europol gone in ensuring that cybercrime capacity building programs are introduced for law enforcement officers in Africa?" End quote.

ALICE MUNYUA: Thank you. Do any of the panelists want to respond to that quickly?

GREGORY MOUNIER: Well, very briefly, on Europol's capacity building programs, unfortunately we're not involved so much in capacity building programs. We really support the member states' investigations. I think that INTERPOL has a much broader portfolio in terms of supporting the capacity building in Africa, for instance, for the cyber criminals, but I think that my colleague from the European Commission has also something to say about it.

CATHERIN BAUER-BULST: Yes. We do find capacity building on cybercrime all prefer the African countries. We've been working for a long time also with the Council of Europe on this, and I have the happy news that there's further funding opportunities coming up, especially for African countries, and we're currently looking exactly at that as cybercrime capacity building.

So good news, I hope, for you.

ALICE MUNYUA: I'm afraid we are running out of time, so I can see we have five -- five people standing to ask questions so I'll ask you to make them really brief, so that we can allow the other speakers to speak, because we don't have that much time in this room.

Please, Tucows. Elliot.

ELLIOT NOSS: Yes. Elliot Noss from Tucows.

Gregory, thank you for that.

Two of my five questions. First, you know, I think you did a good job of identifying that the greatest strength around investigation will be criminals being stupid, and we also know that these are also extremely lucrative big businesses now and the stupid ones

don't stay in business long and are quickly replaced by smarter ones.

I'm wondering, first: Did you also, in dealing with the security community, talk with them about their experiences dealing with registrars and their ability to liaise back and forth with registrars around information?

GREGORY MOUNIER: A very quick response.

I think that -- I mean, I haven't really talked about the relationship with the registrars, but I think the feedback I get from the investigators is that if they have built personal relationships with the registrars, then they tend to get much better cooperation than when they just send requests. That might not fit exactly, you know, is there the lack of background. So that's also something we're trying to do internally to educate our investigators to build relationship possibly with the registrars, and more broadly with the private sector that is holding the key to many investigations, cyber investigations, so that they create a good relationship and so that the private sector knows our constraints, what we're after, and then to the best of their ability can provide with information we need and not everything but just what we need.

ELLIOT NOSS: That's great. I think that that's encouraging and I would describe those as relationships, not necessarily personal relationships, because there's a wealth of data beyond WHOIS that is much more valuable for investigation.

Second question: I did not see on the schedule when you would be presenting this to the CCWG --

ALICE MUNYUA: Elliot, I'm sorry to interrupt you but we are running out of time. We've only got 10 more minutes. Perhaps if you could send us the questions. And I think I'll ask all the other speakers to just ask the questions. The questions can be responded to at the end of the session. Because we're running out of time. Thank you.

Please ask your question but we're not going to be responding to them now. Later. Thank you.

ARTHUR ZONNENBERG: My name is Arthur Zonnenberg from Hostnet. Thank you for the presentation. I'm still trying to understand this foolishness of criminals that you describe.

Indeed, the email address is paramount to catching them, and it is, indeed, often a valid email address because they need it to pay for it. But if I get a set of data from, for example, Catherin over there and I get a copy of a passport from Catherin and then somebody is stealing her identity information, then as a registrar how am I supposed to know that it's not Catherin? The only way I can do that is by actually -- yeah -- asking her "Did you register this domain with me?"

And often we contact people by phone, but even then they can pick up the phone and say, "Yeah, yeah, it's Catherin," and of course we don't know Catherin.

So how am I supposed -- how do you think I am supposed to further validate what we're already doing, fraud checking, various methods which I'm not going to disclose?

And one comment.

I don't object to you getting my data. I object to my political opponents getting my data if I'm active with a Web site against them, but that's the whole activism which we agree to disagree upon, perhaps.

ALICE MUNYUA: Thank you. Can -- yeah. We're not going to respond to the questions right now but you can ask your questions. We'll do

that later. Because we need to allow the other two speakers to present. Yes, please.

ASHWIN SASONGKO: Thank you. Ashwin from Indonesia.

Just want to ask for the two speakers, two previous speakers. In Europe we have some sort of a buy-in to the concept of "know your customer." It means you have -- the bank should know exactly that the customer is this one, and seeing their single ID -- single European ID card, if you can. Also the registrar. If you want to apply for an email, you must know who he is. If a company would like to open a Web site, they must know who they are. Visit their office and check the person. Thank you.

ALICE MUNYUA: Thank you.

Yes, please.

PETER KIMPIAN: (indiscernible). The question is maybe for our European colleagues, it is obvious. For the others, I would say it's very important to emphasize this. For example, Europol is making its job which is accompanied with a very thorough data protection regime. And it is a very high level data protection, especially in

EC3. And there is at Europol a GSB Europol which is fulfilling the data protection investigation of the whole Europol data processing. So there are a lot of expertise again. And I'm returning to what I have already said previously, that are there are a lot of expertise in Europe at the European level that can be valuable in a WHOIS context or so in law enforcement and for the whole structure -- or the future structure. Thank you very much.

WANAWIT AHKUPUTRA: Thank you. I think we need to move on because we will run out of time.

I think next will be the U.K. PSWGs that have been initiating setups.

And I invite U.K. to share with us that apart from the technologies or collaboration works how the procedures and how they organize in each country.

And I would like U.K. to share. We start with Nick Shorey. Thank you.

NICK SHOREY: Hello, there. Right. So I'm part of the U.K. GAC team. I chair a subgroup focused on the public safety working group activity.

Just prior to Internet governance, I was a cybercrime investigator. And I'm also a consumer of domain services and utilizing privacy proxy services. So I see this issue from all sides.

In the U.K., like many countries, we have a wide range of government bodies with an interest and responsibility for public safety that extends to the Internet.

In response to the launch of the PSWG, we brought together all of these departments to consult on the topics. So who have we got? We have CERT-UK, HM Revenue and Customs, who deal with taxation. We have the Intellectual Property Office, the Information Commissioner's Office. We have the medical health products regulatory agency. We have the National Crime Agency and U.K. Policing.

And in addition to this, we've also brought in the Children's Charities Coalition on Internet Safety. And we have John Carr to my right here.

So, hopefully, that answers David's question about sort of the broad scope of public safety and who they feel are sort of relevant to this and have tried to get involved.

So, what is our approach? I think it's critical that governments articulate issues clearly in this area. So my approach has been

to involve practitioners, people working the problem and engaging directly with the Internet community.

Quite often I have found that these practitioners just want a practical solution to a problem. On my left here, we have John Flaherty from the National Crime Agency. John is a technical investigator and a subject matter expert. And he's going to speak to you later about some of the work that he's been doing within the Specification 11 group.

We have been holding monthly meetings in London, discussing work and developing consensus recommendations which then form part of the U.K. response to the PSWG on this.

But I have also noticed it's a great way to share experience and discuss best practice, both for ourselves as government in this area and how we can work more effectively with the Internet community and sort of in addressing these issues.

As Fadi mentioned this morning, ICANN is just one part of the ecosystem of the Internet. And within our Internet governance work, we see this as one element of a broader strategy, participating within the Internet Governance Forum and the Council of Europe as an example.

WANAWIT AHKUPUTRA: Nick, sorry to interrupt. We have two minutes left.

NICK SHOREY: So we'll speed up. Okay.

But we do see this as part of a broad strategy.

We are looking into now going forward to develop sort of day-long workshops. And we would really like to get in registrars and threat response companies to contribute to that. And we do hope this group can facilitate collaborative engagement across government and the community that constitutes ICANN to develop practical and mutually beneficial solutions.

So how can you participate? This is the key thing. So if you are a member of a government public safety body, you can engage with your GAC representative who are present here at ICANN.

The U.K. group, we can also facilitate other members of the GAC in reaching out to their respected public safety organizations. I know it can be very difficult to find the right person. So please come and speak to us, and we can maybe facilitate you engaging with the right person. It might be a G7point of contact or someone from a Council of Europe urgent data preservation list.

And if you are in the wider community, again, you can engage with us directly or through the ICANN processes and collaborate

on identifying practical solutions that are mutually beneficial. I think that covers it. Thank you very much.

WANAWIT AHKUPUTRA: I think we definitely really are out of time. Please, I think -- Sorry. But we have, like, one or two minutes left.

JON FLAHERTY: How fast can I speak?

So Specification 11, as Bobby alluded to earlier, is looking at use, abuse issues around domain names. It came about in response to NGPC and GAC advice around ICANN Beijing.

The quick update from me is an overview of it and who is in the working group, what we have achieved progress to date, and what we're going to discuss this week in ICANN54.

Just to set the scene in terms of why I see a PSWG registry relationship, when I got asked to be a co-chair in this security framework working group, I said, Oh, I have been ringing -- I have been calling registries for years now on cybercrime investigations on U.K. cases, not with requests for information but with a problem.

And it's usually met with a solution sometimes from a registry where technical innovation borders on brilliance.

So that's the current relationship in terms of registries not having to help law enforcement in protecting the consumer but wanting to do that. And I say that whilst fully expecting that not every registry is capable of that kind of response. So I think the framework at the moment is already being practiced. It just hasn't been written down.

So the overview is we are focusing on the use and safeguarding of new gTLDs, gTLD protection, and responding to security threats such as botnets, malware, and phishing. The PSWG is on the outside looking in in terms of how a registry chooses to respond to such security threats. And we bring hopefully best practice case studies to the table this Wednesday in session with registries and registrars to try and see what our engagement is and also post-framework, how we can continue that productive relationship.

The working group is formed of practices and policy people and compliance managers across registries, registrars, and the GAC PSWG working group.

We've now got a voice and a seat around the table to try and influence such a framework. The mutual benefit I think for all parties is that we increase the threat picture overall ultimately to reduce the uptime of things like botnets, malware, and

phishing and reduce that customer harm so everybody can enjoy the massive social benefits that the Internet gives us.

So the update so far in progress this week, we're developing a core security framework. We're each going to submit our idea of what one looks like. I'm working on the principle that less is more. This shouldn't be such a very prescriptive framework. It shouldn't go into too much details. It's got to be very flexible, especially at the technical back end in terms of maybe what certain registries are already providing in terms of an abuse response monitoring and management policy that they have.

We draw on ICANN guiding principles in this process, and they're available in the charter behind this document. Some of the principles are that we must promote industry, timely self-regulations, registry abuse. And there is no one size fits all policy. What works for one registry in terms of safeguarding customers might not work for another.

So we're collaborating on that existing best practice across registries, registrar spaces, law enforcement experience to date.

Finally, the next steps are going to be to draft that framework document, set deadlines with the hope that we can still meet the January 29, 2016 draft document deadline which will then be posted for public comment.

Thanks very much.

WANAWIT AHKUPUTRA: So we are really out of time. We go on with the issues of interest.

John Carr.

JOHN CARR: I will try to do this in about three sentences. Obviously, the child protection, child welfare community has got great interest in a number of the issues that have been discussed already. WHOIS being a very obvious one. But more recently, we became engaged with ICANN when the last round of gTLDs were being created and in particular the .KIDS one. But there are similar ones to .KIDS. Again, I think it's a fairly obvious point to make. If you are going to create a space which ultimately will lead to the creation of Web sites which are bound to attract and are intended to attract very large numbers of children and young people, then it seems to us that there are a number of obvious security concerns which need to be taken account of from the very beginning of the process, and they weren't when the last round took place and we want to try to make sure that that doesn't happen again, should similar things occur in the future. That's why we're happy to be part of this process in the PSWG.

WANAWIT AHKUPUTRA: Thank you. Thank you, all the speakers. And I think -- sorry that we really run out of time. And most of the questions that were asked, I think we will look from the transcript and then we post an answer into the GAC Web site. Back to Alice.

ALICE MUNYUA: You have a question quick. We are not going to respond to now. We will respond online. But please go ahead and ask and then we will close because we have been told the technical people need to get on.

WENDY SELTZER: Thank you very much for the opportunity. Wendy Seltzer. I just wanted to speak very briefly on the issue of public safety. Here as a signatory to one of the comments in the process of privacy and proxy registrations, there was a comment that was written by a number of women and advocates and advocates for those including battered women and abuse survivors. And signatories of those comments were all doxed and had their private information posted online.

Even as we were writing to protect -- to ask for the protection of private information, many of us had to contact our law enforcement to note that this information had been posted online.

And so it's a sort of circular process but I think drove home to many of us even further how the forced publication of information, very similar to that required by the WHOIS, is a privacy invasion and, indeed, a public and private safety concern right there.

ALICE MUNYUA: Thank you very much. I would like to take this moment to thank the panelists and all of you for the great interactions. And we clearly need more than one and a half hours for the next session, perhaps two or three hours.

So we look forward to having another public session at the next ICANN meeting. And thank you very much again.

[Applause]

[END OF TRANSCRIPTION]