MARRAKECH – Registrars and Law Enforcement
Monday, March 07, 2016 – 13:45 to 15:00 WET
ICANN55 | Marrakech, Morocco

UNIDENTIFIED MALE: March the 7, 2016. This is the Registrars and Law Enforcement meeting in Diamant Room. It will run from 13:45 to 15:00 local time.

UNIDENTIFIED MALE: We're going to get going in about another two or three minutes, so hang tight for a moment.

MICHELE NEYLON: Good afternoon everybody. Welcome to the Registrars and Law Enforcement/Public Safety Working Group session. Are we okay down the back? Have you got the recording and everything? Perfect. Thank you.

Good afternoon. I'm Michele Neylon. I'm Chair of the Registrar Stakeholder Group. I'm joined by Graeme Bunton, Vice Chair of the Registrar Stakeholder Group, and then on my left we have Bob. I think you can introduce yourselves. Yes.

BOBBY FLAIM: Hi there. Bobby Flaim, FBI.

LAUREEN KAPIN: Laureen Kapin. Federal Trade Commission, Consumer Protection.

MICHELE NEYLON: And there's a ton of other people around the – we won't [need] to do the entire thing. This is a ton of registrars. There's a ton of you, so we'll just take it from there.

For those of you who haven't been to one of these sessions before, this is I think the fourth we've had over the last few meetings. There are certain areas that are of interest to the Law Enforcement and Public Safety Working Group community and there are areas of interest that overlap with those of the registrars. So we try to come together at these meetings to discuss these things. Hopefully, we can move this dialog forward so that we are collaborative and that we're working on commonly shared goals as opposed to getting bogged down in areas where we will probably never fully agree. That would be a better use of our time. Okay. So maybe, Bobby, you might want to say a couple of words.

BOBBY FLAIM: We appreciate always the opportunity to be here and meet with the registrars and the public community. I think Michele hit it on the head that we're hoping that this session we can delve into some new areas of collaboration and cooperation because I think in the past maybe we've focused on things where we can't agree. So if there's something here that we can do that we can maybe take a new step in a new year 2016, a new CEO, the whole nine yards, I think that would be very beneficial.

I know myself and Michele have privately discussed a few things that maybe we could work on within the realm of DNS and maybe outside that are of mutual interest to both of us, maybe DDoS attacks, maybe working on IP, maybe other types of abuse and criminality where we have a shared and common goal. I think that would be very, very beneficial, and I think it would also be very good for the community.

MICHELE NEYLON: Thanks, Bobby. Just for the idea being that instead of spending our time arguing with each other, we actually try to work towards things that we can agree on. We can agree to disagree on the other things and we'll continue those dialogs and arguments elsewhere, but try and make this a little bit more positive.

So some of the topics, as Bobby said, DDoS. For those of you in the room is there anybody who doesn't have a problem with DDoS? Nobody? Okay. So you all have problems with DDoS. Okay, we can agree on that one. Another one that was suggested was issues around credit card fraud. What was the other one I said? There are a couple of encryption scams that are going around where they basically say – yes, the ransomware encryption stuff. They encrypt all the files, "Pay us."

UNIDENTIFIED MALE: CryptoLocker.

MICHELE NEYLON: CryptoLocker, yes, there are a bunch of those. I don't know. Do other people have areas of interest that they'd like to collaborate on potentially? This shouldn't be the Bobby and Michele show, guys. There's more than the two of us here.

[BOBBY FLAIM]: [inaudible] shy.

MICHELE NEYLON: Okay. Do you want to take the lead on this? You could say a few words of wisdom?

BOBBY FLAIM: Sure. Well, maybe we can start out with DDoS and a general discussion on DDoS. Obviously, that's a pervasive problem on the Internet. One of the things that we have looked at, at the Internet Engineering Task Force (IETF) and also at the North American Network Operators Group (NANOG) is how to do DDoS mitigation.

One of the things that they have come up with at the IETF which we're trying to support and go further with is a Working Group called DOTS, which is an off-shoot of PCP38 where the Internet service providers would be able to do a signaling and inform victims of DDoS attacks, that it's ongoing, and see what ways they can actually mitigate that.

This is a Working Group that just actually got started, I think in the summer IETF, so maybe July, the meeting that they had at the IETF in Prague. One of the things they're trying to work on is case examples, what would be the right protocol on how to do that. So that would be something that would be very beneficial actually to all of us as victims, as investigators, public safety officials. That's one thing.

I know also at the NANOG – the North American Network Operators Group – there was talk that there are lots of reports to

law enforcement and we're not taking enough steps or opening enough cases to address the problem. That becomes a problem not only with investigators because of the multi-jurisdictional aspects of DDoS, but also there are a lot of things that we as law enforcement have to consider – what the damages are, what the legal requirements are, and then if our prosecutors are actually going to take the case.

So one of the things that we were looking to do is maybe have a collaborative effort where we can amalgamate some of these cases as opposed to the onesies and twosies, and approach it as an enterprise level as well.

So those are the two initiatives I think I can kick it off with that we are supporting within the realm of the Internet governance community, not necessarily here at ICANN but at the other, I guess, pillars of the Internet community which are the IETF and the regional internet registries and the network operators. I hope that's enough to kick it off and spur some conversation.

MICHELE NEYLON: Thanks, Bobby. That's helpful. So people – registrars, other people in the room – do any of you have any thoughts? You're normally not this silent. Aha, finally. Rob, go ahead.

ROB [HALL]: Bobby, maybe you can tell us how registrars could help in this, because it seems to me it's an operator and ISP problem typically more than a registrar's. I understand that the DNS sometimes gets attacked, and we run our own DNS servers and we have to mitigate that. The way to solve it often is through the network operators, not us. So how are you looking for us to play here?

BOBBY FLAIM: Just off the top of the head, maybe some of the ways that you as a registrar may be beneficial to a solving of the equation would be intelligence reporting insofar as what you're seeing. What are the modes of attack on the DDoS, and if you're a victim, how would that work with you as a case example that can be provided, especially within the realm of the IETF? Because they are looking for that right now. How are you as victims able to get that information, how do you know you're a victim of the DDoS attack, how is it coming into you, what are the steps that you would take or would like to see taken from the provider as well? Does that help?

ROB [HALL]: You mean in relation to how would we want to report it to you? Because we do see them on our hosting clients. We'll get an

attack against a specific hosting client. So you're looking for how can we better report that to you? Is that fair?

BOBBY FLAIM: That would be one avenue, yes, how you could report it better to law enforcement, but how you can also report it better or raise the awareness within the service providers as well, how you're being attacked and how that information can be shared upstream on the technical level.

ROB [HALL]: Is it perhaps you don't mean the word "upstream" but on a broader community? Because I think most of us, the second we start being attacked, are talking to our upstream providers because they are the key in mitigating the attack often. So they know it. Maybe it's a broader dissemination of that. Is that what you're suggesting [inaudible] to other similar providers that maybe aren't ours?

BOBBY FLAIM: Yes. This is in the very beginning stages at the IETF, so one of the things is trying to determine what is going to be the best way to not only mitigate it, but what are going to be the paths to mitigation. Whether it's upstream/downstream, whether it's

victims that aren't aware or are aware, how is that information going to be shared so the community can collectively address the problem?

MICHELE NEYLON: Just speaking to this, we were the victim of an attack, well, the threat of an attack a few months ago, and one of the issues we ran into was trying to find out how real the threat was because it was one of those things which was obviously going to be part of a bigger series of attacks. So trying to actually even see had this group followed through on these threats in the past or were they just threats. That may seem kind of obvious to some people, but it wasn't to us. Adrian, I can see you nodding. Do you have any experience in this space?

ADRIAN KOSTER: Yes. We saw that kind of attacks also in Switzerland, and we actually made a blog post about threat assessment. The group you mentioned – Armada Collective, I believe, or whatever or DD4BC – usually they just threaten, then they send out a low-level DDoS attack, but they never came back. We posted this from the government side. We informed actually the public about what's the modus operandi of those.

But I think that the main issue that also Bobby is getting to is, law enforcement needs a lot of information. Even if you are disappointed at first at not enough steps are taken, this is basically an Internet crime fighting. You often need big data analysis. Because if you only have one indication of one attack, you have often not enough information to follow up on the leads. So you need to bring several cases together also to assess that this a phenomenon that is not unique, this is not only to one company. Because sometimes when it's only one company, this is a personal matter so you can investigate who is the disgruntled employee who has been sacked a couple of days ago that is mounting an attack, or is it a group that is attacking everyone everywhere? So law enforcement doesn't know what's happening out there as long as you don't report it.

MICHELE NEYLON: Jennifer, go ahead.

JENNIFER STANDIFORD: Hey, Bobby. Michele, thanks for having this session today. This is Jennifer Standiford, Web.com. Just a couple questions. Has this DDoS informative collection of data also been proposed to the registries, obviously, because they're victims of DDoS attacks

just like the registrars? If you could elaborate a little bit more on that just for my own personal information.

And then just thoughts around if the registrars – not speaking on behalf of any of them because I don't want them to attack me in the room – but if a group of us were to provide a set of data, to be defined later, what would be the rights to that data? How would that data be consolidated? How would that data be stored? And then, obviously, what's the intent to use that data – in a consolidated format? To develop trends? If you could just elaborate a little bit more on your thoughts around that, that would be great.

BOBBY FLAIM: I guess the first question is with the registries. What we are trying to do right now, one of the things we're working on is the Spec 11, the Security Framework. This is one of the things that we're hoping gets encapsulated in that framework, so we're currently working on that. I know there are a couple of sessions here at ICANN.

John Flaherty who is from the UK National Crime Agency is our lead PSWG person and unfortunately he's not here. I think he actually arrives today. So maybe during that session, that would be where that would be explained or detailed more.

But just to answer your question and give you how we are talking to the registries on that specifically, one of the things with the registries is to work on more of the security angle insofar as DDoS attacks and botnets, malware, non-content type of information. So that's number one.

Number two with the data, that's also going to be an evolving process. I know with what we do with law enforcement in investigations is we don't collect the data simply for the sake of collecting data. It's always geared towards a direct investigation. There has to be an open case. So if we are collecting data it is for that specific purpose. If we're talking about DDoS attacks, it's to support a case. They may be an aggregation of separate incidents, but it would be for one case.

I know in the FBI – I can only speak for the FBI – sometimes we have what we consider major cases where a crime is occurring in different jurisdictions within the United States, and our headquarters is the coordinator and that's how we would run that particular type of investigation. So it can happen at the local field office or at headquarters if the case becomes large enough. I hope those answered both of your questions.

JENNIFER STANDIFORD: I guess, essentially, yes. But I think that there's additional information to be defined around my concerns around the security of the data and the rights to the data.

BOBBY FLAIM: Well, if we're talking…

MICHELE NEYLON: Sorry, Bobby. It might help, could you speak a little bit to how the FBI do some of those? The releases, the levels of the information, the way they're flagged, depending on the sensitivity and who it's allowed to be shared with. I think that might help speak to Jennifer's query.

BOBBY FLAIM: When we're conducting investigations, it's confidential. A lot of times or most times, the information that we're getting is via legal process. So that is not open. It's locked. Actually, even within the FBI, if it's subpoena or grand jury material, no one else is allowed to see it except for those investigators on the case. So if we're talking about an investigation, say it's a DDoS attack and it's pursuant to a direct investigation, then it would be closed information. It's not public information. It's not released, and it would be safeguarded.

JENNIFER STANDIFORD: Thank you.

MICHELE NEYLON: Go ahead, Mohamed.

MOHAMED [EL BASHIR]: Thank you. I have two question. The first one is regarding the jurisdiction and who might be concerned. If you are a registrar who is not based in the U.S., for example in Africa or somewhere else, and you get a DDoS attack and just want to file the case, what's going to be our interface in order to submit something? This is the first thing.

The second one is in terms of cooperation because the case is if something happens in one country and they don't have this type of cooperation between the law enforcement locally in that country and the people who are making the attack from another country, so what type of cooperation that we have right now setting up between law enforcement between different countries in collaboration with the registrar to collect or to try to get [in order to] try to work together to understand better the case and file something? If [we live] in a country that's very weak and doesn't have a strong mechanism in terms of law

enforcement, so what has been discussed now in order to get these things sorted out?

BOBBY FLAIM: Yes, I think your first question was if it's a cross-jurisdictional crime – so the perpetrator might be in one country and we're investigating in another – how do we address the problem? There are two ways we can do it. The first way is what we call the Mutual Legal Assistance Treaty. That is kind of a long bureaucratic process where we would request through our Department of Justice evidence through legal process of another country of another ISP or organization. That's one way. The other way we could do it is actually open a joint case with our international partners where, if there was the FBI and we see the case is coming from Germany, we can open a joint case with the German police and be able to share information that way. So that would be question number one.

Number two, let's talk about greater collaboration and international efforts with cybercrime. We have two things. The first thing is the Cybercrime Convention, which I don't know how many signatories we have but we have quite a few – I'm going to guestimate the number is about 50 – where we are trying to develop coordinated cyber internet crime laws across jurisdictions.

The other way is we also have Interpol and Europol here that actually works with the individual member states – we have Kimmo from Interpol and Greg from Europol here – where they work with their individual member states to ensure that the cybercrime laws are consistent and if they're not, how would they work with their membership? But if they have anything to say, I don't want to speak for them. But that's also another way to do outreach, work collaboratively on an international level as well.

KIMMO ULKUNIEMI: Kimmo Ulkuniemi from Interpol Global Complex for Innovation. This kind of information request they are always difficult, like Bobby already explained. If you need to use the information as an evidence, then a mutual legal assistance treaty [inaudible] request is the only way to get the information. In law enforcement, we know that sometimes you are not able to get any evidence that route. Sometimes it might take two years, sometimes three years to get evidence.

But in most cases for law enforcement, it's okay to just have information for intelligence and [inaudible] investigation. In these cases, for example, you can use the Interpol. We have offices in 190 member countries. You can request information from one country or another country, and this information

cannot be used as an evidence, but to [inaudible] the investigation.

It also depends on national legislation what kind of information you can request, and that always is not clear. Bobby already mentioned the Budapest Convention on Cybercrime. I think at the moment about 40-45 countries signed the Budapest Convention. It's one tool which provides you a way to request information, but still there are around 150 countries who don't have a Budapest Convention or any kind of information exchange framework for these kind of cases.

GREGORY MOUNIER: Hi. Gregory from Europol and the European Cybercrime Center. In Europe we have the European Cybercrime Center, which means that if we receive information which has been gathered by the law enforcement authorities of one of the 28 member states or one of our corporation [partners] like the US, then we don't need MLATs. We can share evidence within our jurisdictions or Cybercrime Center which makes the whole investigation – a cross-border investigation – much more efficient.

We have pan-European databases, so if you guys were to have interesting information on a DDoS attack, for instance, or if you

suspect that there is an organized crime group, like what for our Swiss colleague mentioned the case of DD4BC, it was clearly an organized crime group operation at global level that was attacking financial institutions and other enterprises, and then if you send the relevant information to either your local law enforcement and they send it to us, then we can cross-check everything into a central database. Then we can make links between the various operative cell, I would say, of the same organized crime group.

So for us really, we're not conducting proper investigations, but we are connecting the dots between various investigations that are ongoing in the various member states. That's really the added value of having this type of structure like Interpol or EC3. Again, I think it's really important this type of public/private partnership. I know it's [inaudible], but the more you share with law enforcement, the more intelligence you share with us, the more we can help you to identify who is behind those that are attacking you. So, yes, I think the structures are in place. You just have to make use of it.

MICHELE NEYLON: I can see hands up down the back, if you want to come up to the microphone.

CAITLIN TUBERGEN: I have a microphone back here.

MICHELE NEYLON: Oh well, Caitlin, you have to stand up.

CAITLIN TUBERGEN: Hi, this is Caitlin Tubergen speaking on behalf of remote participant Chris Pelling. The question is, "Whom to report to then? In other words, can we get a list of e-mail addresses or persons, etc., and can this be provided to the Registrar Stakeholder Group?"

MICHELE NEYLON: You may need to repeat that, Caitlin. It wasn't very clear back here.

CAITLIN TUBERGEN: The question is, "Whom to report to then? In other words, can we get a list of e-mail addresses or persons to report to? If we can get a list of persons or e-mails, can it be provided to the Registrar Stakeholder Group?"

BOBBY FLAIM: Yes. I think for starters you could definitely use the people that are on this panel, since we have Interpol, Europol, the FBI here. I think that might be the first start. I know for the FBI in the United States, we work with our state and locals. We also deal with a lot of our other international partners, but I think maybe also for Europol and Interpol, since they are international organizations, that might be the first start. But again, I'll…

MICHELE NEYLON: Maybe you might want to follow up with me later and give me something, and we can then work from there. That might be a little bit easier.

BOBBY FLAIM: Absolutely.

ADRIAN KOSTER: Let me just jump in there. Every one of you is located somewhere, and there you have local police. They often are not so aware of cybercrime and how this can be reported and everything. But more and more countries at least at the national level they have cybercrime-competent centers. So go and find out in your country which is a competent law enforcement authority where you can actually report or where you can talk to

and where you know that they understand you and your issues. Because if you go to the local police station, they might be able to refer you to a specialized unit, but they themselves might not be able to understand you in a way that is helpful for you. But they can certainly direct you towards a competent unit within the country, because that's a jurisdictional issue.

BOBBY FLAIM: The other thing I was going to recommend, since we are at ICANN, is from your respective governments – and I know not all of them are here, I know Michele has had this problem – is to actually talk to your Governmental Advisory Committee, or your GAC rep who are supposed to be coordinating with their law enforcement and consumer protection and public safety agencies back home on these very issues. So that would be, to follow up with what Adrian was saying, to deal with your respective national government GAC representatives but more particularly with your law enforcement representatives as well.

MICHELE NEYLON: Kimmo?

KIMMO ULKUNIEMI: Yes. I wasn't sure if I understood the question, if it was about reporting of crime or if it was just general information about law enforcement. When it comes to reporting the crime, unfortunately Interpol or Europol, we are not the agency you should contact. It's always the local police. I can speak on behalf of my colleague from Europol. They have an excellent website. You can get information how to report crimes in European countries hopefully. In the future, we are going to have the same in Interpol level also. But certainly, I think we are here with all the colleagues from law enforcement, and if this need to discuss about project how we can work together and cooperation in general.

MICHELE NEYLON: Thanks, Kimmo. Sure. Just go up and grab the mic. While she's walking up, I think the concern I suppose is for a lot of the registrar members we have, they're operating in multiple countries. I know some of them own multiple companies who operate in multiple countries as well. So something that's easier and more accessible rather than talking with the local police, which may not help when you're running operations from the other side of the world. I think that's part of the problem. Thank you.

Sir. Please state your name for the record.

FABRICIO PESSOA: My name is Fabricio Pessoa. I'm from Brazil. I work for AXUR. That's a private company, and we deal with phishing, malware, and this kind of stuff. Now, by the end of February, I was in San Francisco for the M3AAWG event. One of the topics was exactly about that and how to report things for law enforcement.

Because sometimes it's difficult for us to know when we have a case for you guys. We know that you guys have a lot of things that you have to be worrying about and we have lots of information. But basically usually it goes from, for example, we detect and [ask] and try and have the take-down. So it's a direct communication between the hosting provider, the ISP [inaudible] and us.

Most of the times, because we deal with the malware, phishing, and things like that that, we have so many, it doesn't even get to law enforcement. We resolve it by ourselves.

However, I think it's data that we are collecting, and it's not being used. It's just between us, and we are never try and get the root of the problem that is the bad guys that are doing the things. Right? I've tried personally to talk to Interpol and FBI and offer this data, and nobody seems to be interested in that.

So I know that maybe this is not the priority, but I think that something could be discussed. Try to find a way of getting all this information and try, as you said, to connect the dots. Maybe you are not going to be looking after all the guys that send the e-mails, but if you see a pattern or something like that, you could do something.

I'm sure that most of people that work in the industry would be willing to share this with you guys as well, because for us the sooner we get the things down and the sooner we get the guys, the better. But I think that there is a gap that we have to fill there and maybe start discussing more, everybody, all the actors involved. We are trying to sort it out between us, but I think that maybe when we get better organized, it would be nice to have you guys jumping in as well so that we can make it broader. Thank you.

BOBBY FLAIM: Thank you very much, and we can definitely meet after this meeting and exchange information. That would be very beneficial. I know for the FBI, a lot of case development is working with private industry. I know when we did our GOZ CryptoLocker case about a year and a half ago, that was in direct cooperation with our private partners, so absolutely.

MICHELE NEYLON: Ben?

BEN ANDERSON: Yes. Thanks. Ben Anderson, NetNames. I guess for me, and to echo that gentleman's point, I think what would be helpful is for you guys to [club] together and provide a toolkit of some kind, instructions on what it is that we should be providing in order for you to have a forensic investigation. Because you're talking to lots of different registrars from lots of different places who operate on various different systems.

I think the ultimate goal is that I'd like to provide our engineering department with a list of things that you would want to see. We can discuss where that's submitted at a later date, but ultimately is what do you want to see so you can conduct a forensic investigation to help with the wider problem? Because without that, then we're all going to start doing things in our own unique way, which isn't going to really help. So we would look to you for guidance and a toolkit to help assist in submitting that evidence.

BOBBY FLAIM: Thank you. I know that after one of the last NANOG meetings, I think it was a year ago, they asked for something very specific. We have started working on it, but with the bureaucracy, we're still working on it. But it's a very well-taken point, and we are definitely trying to finalize that.

BEN ANDERSON: Yes. I think you'll find that even though you deal with bureaucracy, all the different registrars within this room will probably want to do things their own way, which is equally as confusing.

MICHELE NEYLON: Okay, I'm going to pass the baton briefly over to Graeme on my right.

GRAEME BUNTON: I think actually we were in this discussion, we can segue into a two-part piece, which is, how can we help you with national governments? And I think there are two pieces to that. One is participation in this space. And then the other is helping provide you with the tools and the clarity that might be coming from national legislation, and how we can work together to find compromises there. So what are the pieces that registrars can

help with to get law enforcement what they need to participate effectively here and to participate effectively at a national level with us?

MICHELE NEYLON: And thousands died in the rush. You're normally not this timid, Bobby.

BOBBY FLAIM: Okay, I'll start. So, Graeme, for your first part you said what can registrars provide to law enforcement to get what they need? I think going back to what Ben said, maybe it would be good to have something that we provide that might specify– not necessarily how we do investigations because each one of our law enforcement agencies do a little things different – but what would be good for case development? What are the specific types of evidence that we would need and the information, the data, that we would need to actually build a substantive case that we would actually be able to present to a prosecutor? I think that might require some back and forth, but I think it's definitely something that would be very productive. And if any of my other colleagues wanted to add anything.

Maybe it's the after lunch. Everyone ate and drank.

MICHELE NEYLON: So, basically, what the FBI says goes for everybody, and they're all happy.

GRAEME BUNTON: Maybe I can make this a little more focused by throwing my own country under the bus. Tucows is Canadian. I'm Canadian. We operate out of Toronto. I know there is a Sûreté du Québec member who participates occasionally at ICANN, and I know there is an RCMP member who follows this occasionally. But they don't appear to have the resources to participate in ICANN or the DNS world or Internet governance fully.

I've had conversations with them to see what we can do there. But I suspect that's not an uncommon problem for law enforcement to be able to have the sustained presence within this space that requires considerable amounts of time, energy, money, just to get up to speed, understand, and then be able to participate effectively. And so I would love it if the RCMP were here and we could engage, they could understand our local problems, and maybe there's stuff that we could all learn from that.

The question is, how can we help you guys work with your own national governments, your own law enforcement bodies, to

gain the resources you need to be able to participate in this space?

BOBBY FLAIM: Okay. That's a very good point. Well, one of the things that we've done, and we're hoping that this starts to help – you are correct, resources are very scarce. I've been very lucky in my organization in that I'm the only one who started off on American Law Enforcement across many, many, many law enforcement agencies. We have 20,000. But to come to Morocco or other countries and participate, especially when you have a full-time job, it's not easy. It's collateral duty.

One of the things that I've always advocated for – not just for my own organization but really throughout law enforcement – is to have a person who's dedicated to more of a strategic view of the Internet and Internet governance. That we're working on. It will not happen overnight.

But one of the things that we are or have done that has improved the dynamic is the actual creation of the Public Safety Working Group because now a lot of law enforcement have the ability to engage in something that is very concrete and very visible. A lot of times in the past when we said we're coming to ICANN, the justification was like, "To do what? To see who?

What's the primary purpose?" I think with the creation of the Public Safety Working Group, we have gone a little bit further in an actual development or a formal body that law enforcement and Consumer Protection and other public safety working groups can participate in.

Now we've created the pool, we've led the horse to water, it's going to be up to those individual agencies to come. Now where you can help as the registrars is you can go back to your own law enforcement. The RCMP is like, "Look, we keep hearing from the FBI, why aren't you there? Why aren't you participating?" And that would go from Michele Neylon in Ireland and so on and so forth. How do we broaden the approach of law enforcement so that more of them are here? We definitely have been working on that for 10 years, but unfortunately it ebbs and flows.

One of the great things is that we do have now the European Commission, that has Tjabbe there, that have come consistently. We have Kimmo who's been coming for the past couple of years very consistently. We have Europol that's been coming. So we are trying to approach it as a more diversified, populated, and consistent approach. But unfortunately, that is going to take a while. I know like I've said a million times, people are tired of seeing me, and I begged and pleaded and marketed to have more participation from law enforcement, but we just

have to keep trying. But if you can add to that, that would be great.

GRAEME BUNTON: I guess to be quite honest, the more law enforcement is able to participate and understand, the less problematic issues can be. We can have clarity and ease of communication. So greater participation we generally think is excellent, and we love to see the creation of the Public Safety Working Group. That's great. So maybe there's like, for many of us because the registrar constituency is very diverse – we've got members from all over the world – maybe it's even a pitch document from the Public Safety that we can then bring to our home constituencies. We can get it translated, and we can move forward with helping you guys gaining membership and being able to participate.

BOBBY FLAIM: One of the things she's also done – Iranga is also from the FBI and works in our office of National Policy – one of the things we've also done is actually to try to come up with a pamphlet that we can give to our international partners as well. So we are working on that where we can talk to the heads of government to say, "Look, this is a priority for Interpol, for Europol, for the

FBI, for the Federal Trade Commission, for the European Commission, and it should be a priority for you as well."

MICHELE NEYLON: Thanks, Bobby. Any of the other registrar colleagues want to weigh in on this topic? I'm amazed by the silence. It's definitely this post-lunch thing, Bobby.

UNIDENTIFIED MALE: We're more used to shouting at each other.

MICHELE NEYLON: Yes. This is kind of LEA 2.0. They're warm, they're cuddly, they're fuzzy, it's a whole new uncomfortable situation.

Graeme, did you have another topic that you wanted to raise?

UNIDENTIFIED MALE: [inaudible]?

MICHELE NEYLON: No, I don't think so. No. Not immediately. Okay, so there was another topic that, I think I'll let Graeme broach this because he's a polite Canadian.

GRAEME BUNTON: This one might be challenging and probably maybe should have been discussed with registrars previously, but we hear a lot about "bad actors" in this space. I'm going to throw that in quotes, because it's a phrase we hear often, frequently. It's repeated all the time, "bad actors." That's somewhat frustrating, I think, for us. And to be very blunt and horribly unpolitical, it's often used, I think, as leverage against the rest of the people probably in this room who are generally the good actors.

I think maybe we can, in working with law enforcement or public safety, be more specific about who those bad actors are so that if we have a narrow problem in a narrow jurisdiction or a specific group of people, then we can actually talk about them with some specificity and not just use it as a sort of vague term of bad actors. That does two things. It makes us feel a little bit better about the people who are participating and trying to be good, and it helps us maybe solve a problem and we can tailor solutions more narrowly rather than try and tackle a very broad issue that's going to impact everyone in the room.

[LAUREEN KAPIN]: Thanks for that. What I hear, your concern is being tarnished with a broad brush and that sort of terminology not being very helpful because it's not specific and if it's not specific, what are you to do? I have a couple of responses to that.

First, I'll say that the activities going on with the exploration of voluntary initiatives and the healthy domain name initiative, I think is a positive development. I know my colleague Iranga actually participated in the inaugural Healthy Domains Initiative meeting in Seattle, and from what I've read about what went on at the session, it sounds like a good start. It sounds like there's a lot of constructive dialog going on, and I'm eager to hear how that develops.

I think one response to this broad brush tarnishing that you're concerned about is the antidote sometimes is broad, good behavior, and exploration of initiatives like this to see what can be done in terms of making efforts to create a healthy ecosystem. So I think that's all to the good.

From a practical perspective, I can't talk about any specific situations because you're not really talking about a specific situation, you're talking about a general topic, but I can say in law enforcement, whether it's on the civil or the criminal side, if

there are investigations going on, often they're confidential and information can't be disclosed until you're at the end game where things are public. So in terms of timing, there's always going to be a sensitivity about being able to get very specific until after the fact.

But my sense is that you're not really talking about that sort of timing issue. I think you're talking about language or attitudes that aren't very productive because it's so broad and so negative that it's not useful. And I agree with you. I don't think that sort of discussion is useful. I think you need to come to the table with an open mind. And, as Michele says, sometimes we're not going to agree, but that doesn't mean there aren't going to be a lot of areas that we can collaborate on and make some progress in. And I think that's a much more constructive attitude for meetings like this.

MICHELE NEYLON: Okay. Thank you. The idea ultimately is that we're trying to make these dialogs more constructive, and we can save beating up Bobby for later. Jokes aside, there are a couple of things. When you did mention the Healthy Domains Initiative, this is something that is not being driven by the Registrar Stakeholder Group. It's something that some of our members are involved with and some of the registries are involved with. I think even

some of the CCTLDs might be involved with because that's being run by the DNA which is not us, though there can be an overlap.

Also, I know some of you were at an anti-abuse thing we ran in Dublin. We had another meeting yesterday, and so some of your colleagues are engaging with us there. We're trying to have some kind of conversations just to see if we can move the needle in the right direction on some of these topics. Nothing binding or anything like that, but just trying to make sure that when you want to yell at me, you're yelling at me not at Graeme and vice versa. Him being Canadian, it's much easier to yell at him. The phone calls are cheaper.

Graeme, did you have anything else? No. Bobby, did you have anything? Please, Kimmo, go ahead.

KIMMO ULKUNIEMI: Yes. Just a follow-up question from Dublin. I believe it was the registrars who said in Dublin that you're preparing some kind of information package, and that would be extremely useful for some of the law enforcement organizations.

GRAEME BUNTON: Sure. Yes. You're right. We talked about a sort of standardized abuse reporting document in Dublin, and we've been working on

that since – maybe not as hard as we possibly should. So to give an update for the community, we're still working on that within the registrar community. I find we're alternating between too broad concepts and then too prescriptive action, and we haven't quite found the right balance between those two things so that we can provide a document that provides clarity and structure for abuse reporters while it still maintains the high level principles that it should. I'm hoping this week to inspire the registrars in the room and the registrars here in general to participate more. We can through another round of edits, and then we can hopefully share that more broadly and then begin to get feedback from the community and clean up some of the rough spots and get that out into the wild.

I had thought it would be a much faster process than it has been to do that, and some that's my own fault for not dedicating some time. But I think at this meeting we've got a little bit more impetus. We can hopefully get through another round and get that out. If people want to approach me directly, I'm happy to send them a draft of what is with several pages of provisions, of "this is clearly a document in flux and has undergone serious edits and will undergo many more."

MICHELE NEYLON: As Graeme mentioned, this is something we have been working on for quite some time. We have members with different business models from all over the place, so the more that they get involved with this and discussing this – I mean, come on, you guys are governments. How quickly do you agree on a treaty? Put it in that context. We're not quite governmental, but it can be a little bit slow.

Any other topics from anybody? Jennifer, please go ahead.

JENNIFER STANDIFORD: Thank you. So, Michele, you mentioned that the Registrar Stakeholder Group wasn't associated with the HDI or the DNA initiatives, but I'd just like to give a plug for the HDI event that's coming up on…where's Mason…Mason? Anybody? Wednesday at 10:45 in the morning. There were some good activities that came out of the Summit in Seattle that was held last month, and one was around the standardization of an abuse report form, and coming from my registrar, I like standardization. So I think if that's something further that we can discuss around a predictable model regarding what you're looking from a reporting perspective and in a format that makes sense, it's at least a good place for us to start.

MICHELE NEYLON: Okay, thanks Jennifer. Around the standardization discussion, the meeting we had yesterday which is taking in a much broader base than registrars and registries, because let's face it if you can't get to the hosting providers, the cloud, the data centers, the people running the IP addresses, etc., it's a bit pointless. We're discussing coordinating that a little bit. Jay? I'm going to pick on Jay. I like picking on Jay. Picking on Jay is fun. Jay, would you like to say a couple of words on that? No? Maybe?

JAY [SUDOWSKI]: I don't know what that is, to be honest. I was sending an e-mail.

MICHELE NEYLON: Thank you for your honesty. What he would have said if he hadn't been sending an e-mail is that the Internet Infrastructure Coalition has been trying to act as a kind of a coordinator to a certain degree around some of this. There are several initiatives going on in parallel that can be complementary, so part of what we're looking at, at the moment over there – which again, as I say has nothing to do with the Registrar Stakeholder Group necessarily, though there is overlap in terms of the people involved – is trying to get a better view of what work has been done, what work is ongoing, who's doing it, which gaps there

are, and where there is overlap. And that's exactly what Jay would have said, but he didn't.

JAY [SUDOWSKI]: Absolutely. I agree.

MICHELE NEYLON: Thank you. So there is some work that's going on that's helpful that hopefully will help us all. Any other items here, or should I give you back 20 minutes? Okay. I'm going to give you back 20 minutes. Thank you everybody, and see you around throughout the rest of the week. If any of you would like to swap cards or mingle with the registrars, there are loads of them here. Thank you.

[END OF TRANSCRIPTION]