DUBLIN – Role of Voluntary Practices in Combating Abuse and Illegal Activity
Wednesday, October 21, 2015 – 10:00 to 11:15 IST
ICANN54 | Dublin, Ireland

ALAN GROGAN: Hi, I'm Alan Grogan. We're going to start the session. This is being recorded and translated, just so you're aware.

Welcome, everybody. We've got a large panel. I'm going to try to keep this moving pretty quickly so that we have time for questions at the end. The topic, as all of you know, is Voluntary Practices in Combating Abuse and Illegal Activity.

One of the things that I've done since I took over this role a year ago is try to explore ways that are outside of the contractual compliance realm where ICANN could play a role in facilitating or encouraging the solution of some of the difficult problems that the industry faces. So what we're going to do today is talk about what ICANN's role is, provide an overview of voluntary practices, and the role that they've played in addressing illegal activity and abuse in various industries, including the domain name industry, but not limited to that.

We've got a panel here that can discuss specifics of some institutions that have been successful in doing that, and then open it up to a general discussion.

So, ICANN's role. As Fadi said in his opening remarks, ICANN can't be the solution here, but we can be part of the solution. Despite what some people in the community would like us to be, we're not a global regulator of Internet content. ICANN's mission statement is actually pretty narrow.

We have a limited, largely technical remit, which is to coordinate at the overall level the systems of names and numbers and protocols that allows for an interoperable, unified, worldwide Internet – a very important role, but quite a limited one in terms of technical scope. And as Fadi showed in his opening slide, our role is mostly limited to the logical layer that relates to making the Internet work.

We're not vested with the authority to act as judge or jury or make legal determinations. We're not vested with the authority by this community or by countries around the world to impose remedies for violations of law, and really building solutions to police illegal activity and abuse is outside of ICANN's remit and mission. But I think there is a role for us to play.

I think we can encourage and cooperate and facilitate with various members of the community who are working with other institutions to try to solve these difficult issues. We can potentially participate in efforts by other institutions to help solve some of these difficult problems, but we always need to be

mindful that we need to do that in a way where we stay within ICANN's limited mission and remit.

Overview of Voluntary Practices. I'm going to provide just kind of a general introduction, and then the panelists will describe how what they've done fits within this.

I think, broadly speaking and probably oversimplified, there are two different approaches to voluntary practices. One is private negotiations between parties have resulted in either binding commitments or MOUs or understandings by parties to take certain actions when complaints are brought to their attention. And those agreements or commitments may be public, but often they're private and confidential.

Often there are negotiations that lead to an understanding that people will take action, but the criteria under which they agree to take those actions remains confidential. Ultimately, it's up to the party to decide when it's appropriate to take the action.

Then there's another category, and some of the spam and malware block lists that all the people in this room are familiar with probably fit into this category, which is there's no formal agreement, there's no commitment, there's no binding undertaking, but there is reliance on data that's provided by trusted sources. And people voluntarily agree to take action and reliance on that data because they think it's in their interest or in

the interest of their customers and consumers to rely on that data and take those actions. So what do voluntary solutions have in common?

When they're the results of negotiations, the negotiations sometimes are convened by a trusted third party that acts as an intermediary or a mediator. Sometimes they're just bilateral negotiations between the impacted parties, the party that's trying to find a solution to a problem and the party or parties that they believe can help them solve that problem. The goal at the end of the day is market-driven voluntary self-regulation.

For those negotiations that have resulted in successful frameworks, the negotiations have frequently taken years to complete, and the solutions that are ultimately implemented for some of those negotiated solutions often rely on a trusted third party, either for the data that they rely on or for the implementation of the solution.

So why do people adopt voluntary practices? If they're not mandatory, why would you do it? I think there are several reasons.

One is, depending on the circumstances and the facts, sometimes there's potential liability, so parties that have self-interest in trying to avoid legal liability. Sometimes it's reputation. Sometimes it's a desire to do the right thing.

Sometimes it's financial. There are a lot of different reasons to do it, but they have been implemented in a number of industries.

I'm going to launch into a panel discussion. I'm going to do just a quick ten-second introduction of the panelists, and then turn it over to them.

The panelists are from the Center for Safe Internet Pharmacies, Marjorie Clifton, who somewhere back there. Center for Safe Internet Pharmacies is a nonprofit that's working to try to address the problem of illegal pharmacies online. I'll let her speak more about that.

John Horton, who's the CEO of LegitScript. LegitScript is also at work to try to solve the problem of rogue or illegitimate online pharmacies, and he works with both CSIP with Marjorie and with the Alliance for Safe Online Pharmacies.

Kristof Claesen is policy and public affairs manager of the Internet Watch Foundation. That's a global hotline combating child sexual abuse material online.

Toe Su Aung, who's the founder of ELIPE Limited, which acts as a — Toe Su's over here — as a policy advisor to the International Chamber of Commerce BASCAP, the Business Action to Stop Counterfeiting and Policy.

Tom Dailey, who's sitting next me. He is currently VP and General Counsel at Verizon International. He served in the early days as the chair of the Center for Copyright Information, which implemented the copyright alert system, a voluntary system by which copyright owners send notices to participating ISPs in the US, and notices are forwarded to ISP subscribers in a series of graduated, escalating copyright alerts.

Roman Hüssy, who is the security [reacher] and head of Abuse.ch, a nonprofit that provides tracking of botnets and malware.

Benedict Addis, who is a member of our Security and Stability Advisory Committee, and he's involved in two efforts. One is the nonprofit shadow server foundation that gathers, tracks, and reports on malware, botnets, and electronic fraud. And then his more recent project is the establishment of registrar [of] Last Resort, which is a special function registrar that was recently accredited. Its goal is to house malicious domains that have been subject to takedowns as a result of botnets and other malicious activities.

And then Dave Piscitello, who is somewhere. Oh, back there again. He is VP of security and information and communication technology coordinator at ICANN. He also serves on the steering committee of the Anti-Phishing Working Group, which by the

way, although it's called a working group, don't get confused. That doesn't mean it's an ICANN working group. It's a separate non-profit that works to resolve a variety of challenges to address issues of cybercrime.

Frank Collin, who is Executive Director of the US Chamber of Commerce Global Intellectual Property Center, and he's here to speak about how a number of members of the US Chamber of Commerce try to address voluntary solutions to combat illegal activity and abuse as opposed to regulatory or legal action to do that.

And Bertrand de la Chapelle, who a number of you know. He's a former ICANN board member and co-founder and director of the Internet and Jurisdiction Project, which is an ambitious undertaking to try to solve transnational cross-border issues relating to issues like domain seizures, content takedowns, and access to user identification.

I'm going to turn this over to Marjorie and John. Who wants to go first?

UNIDENTIFIED MALE: Where is Marjorie?

MARJORIE CLIFTON: I'm right here. I kicked poor [Dan] out of his chair. It's a crowded space in this voluntary initiative world. Do you want me to go ahead and start?

ALAN GROGAN: You go right ahead. I'm going to have swap out a drive here real quick. It'll probably hate me [doing that].

MARJORIE CLIFTON: Alan, what's the easiest way for us to forward these slides [inaudible]?

ALAN GROGAN: I'll do it.

MARJORIE CLIFTON: Okay. Thank you, first of all, for having us. My name is Marjorie Clifton. I'm the Executive Director for the Center for Safe Internet Pharmacies.

Given that there's a lot of people here to talk, I really want to just spend today focusing on the successes we've seen, because I know that this is a really challenging space for all of you. We see this, and our organization has been trying to help navigate the Wild West of the Internet.

We started in 2010, and we include organizations that we call Internet intermediaries. This includes registries and registrars, search engine advertisers, shippers, payment processors, anyone who's involved in the search and purchasing and shipping of, in this case, prescription drugs.

The reason prescription drugs became its own category, in a way… We were modeled after NCMEC, which most of you already know (National Center for Missing and Exploited Children). The reason being is because there were deaths associated with prescription drugs and counterfeit drugs being sold online.

We are happy to provide a lot of information about what the scope of the problem looks like, how it's impacting consumers. Right now the stat from the FDA is that 97% of online pharmacies at any given time are illegitimate, meaning that they're not following the laws of the country that they're selling in or to.

Because of that, in partnership with the White House, they brought companies together, which include many of those here today – Neustar, Rightside, and GoDaddy – who are very active and supportive members of our board, and have really been instrumental in also putting together what now is our principles of participation, which is an outlined document that basically

speaks to how different companies and different sectors are going to address this issue of illegitimate online pharmacies.

I think Alan touched on this in a good way: why does it matter? Obviously, there's liability issues associated with these kinds of things, especially when it comes to things people are consuming and could potentially kill them. What we also know is that physicians are largely unaware of this problem, so in a lot of cases… We're seeing a lot of people being pushed that direction, and consumer audiences not really understanding the space.

Our mission really is about education. That's consumer education, but it's also sector education. I spend a lot of time at conferences helping companies like ours on our board. You can see them up on the screen right here; we're 13 different companies, intermediaries. And information sharing between companies, focusing on what are the best practices and the ways that you can do this that, frankly, will cost you the least amount of money, will cover you in terms of liabilities, but also will give your company a good name in the consumer market.

Those are the three areas we're focusing on. And the other is this advocacy and communication piece. That has been helping not just our industries, but all of the people we touch in law enforcement and federal government and regulators and others

understand the perspective of our companies, frankly, why it is that we can't just turn the Internet off one day.

As we're going now globally in the EU as well as in Asia, talking about this issue and trying to address it, we're having to have a lot of dialogue to help people understand, frankly, what a registry and registrar is, and why you can't just flip a switch one day and make all the bad problems on the Internet go away.

A big role that we're playing is facilitating that dialogue and helping federal government understand how businesses work — I know that seems shocking, but not everybody in government has worked in the private sector or understands that point of view — helping law enforcement understand, again, what you need as cover when you take action on a site as our companies do, things like that. So that's really what we are focused on.

Alan, can you forward for me? I've covered a lot of this, so I'm going to keep going on slides, because what I want to focus on is where we've seen successes. Again, what we're trying to do is hit these illegitimate pharmacies at different choke points.

For payment processors, that means stopping payment. For search advertising, that has meant eliminating illegitimate ads that are appearing on the search engines, and for all of these different… So this is not just registries and registrars. This is

everyone who touches this space, because we do see this, not only as an industry collective, but also as a global collective.

If we don't address this on a global platform, it will never end. And a big piece of that, by the way, as we hear from law enforcement, as we hear from governments, as we hear from everyone, is consumer education. We do feel that there is a consumer piece to this, and that when and if consumers have good information, we can help redirect their choices. It can't all just fall on us as industry. Next slide. Keep going.

And we are happy, by the way, to make any of these slides and this information available to you. I'm always available. Statton Hammock from Rightside is on our board; James Bladel from GoDaddy. Jeff Newman formerly was on our board, so they can track me down if you need to find me.

Again, these are a lot of statistics about impacts. Right now the World Health Organization talks about 100,000 deaths a year related to illegitimate online pharmacies and how difficult it is for consumers.

One of the things we have coming out through CSIP… It's hard for consumers to know what is real and what is not. We have data that's actually coming out this year that illustrates who the consumers are, and much to our surprise, they are hyper-educated, they have higher incomes, and they think they're

smart enough to know. It's not actually the consumer we would think it is. It's actually informed consumers. So that tells us a lot about the kinds of education that we need to be doing, the ways we need to be educating consumers.

Next slide, please, and keep going. I know we've got a lot of people to speak, so I don't want to crowd the space.

The principles of participation. Industry loves best practices documents. That sends everybody running with their hair on fire when they hear that. But we did manage to get our respective sectors to work together to come up with some top-level "here's what we know is working," and that is now spreading globally. Again, it's about having very defined ways that you can protect yourselves, but also know when and where to take action. Next side, please.

The success we've seen is that in last year alone we shut down over 9.6 [million] illegitimate online pharmacies. That is a collective of all our board members together, and that's pretty significant. That number has risen in the millions every year, and we hope that means that we're getting better at what we do, and we also know that the problem has not slowed necessarily, so it means that we have to continue getting better. Next slide, please.

One of the things we also do at CSIP is to facilitate law enforcement action. We've been able to see a lot of… Not bang for our buck, but impact for our time in working with international law enforcement on Operation Pangaea, which is a short duration of time, and it means that our companies are taking action on very specific sites that are brought to them that are part of an operation that last year accounted for $81 million US dollars worth of dangerous medicines, 156 worldwide arrests — you can read the slides for all the rest of the statistics — but I think the key thing is it's about getting to the core of criminal networks.

Instead of it being a whack-a-mole project, how do we get to — and what we hear to be true is that there is a limited number of criminals who are operating a lot of these different sites, so how do we find out a way to get the hubs that are producing a lot of this activity? Next slide, please.

Another thing that we have done is created search engine ads whereby we have about 300 different [pharma]-related keywords that we know consumers to frequently search. By the way, we're doing this in the EU in lots of different languages now as well, the goal being to provide consumers with good information when they go searching for a pharmacy. What we've seen has been really surprising, which is that consumers are in fact looking for good information, because the click-through

rates on our ads are higher than average Google or Bing search ads, significantly higher.

We've gotten a lot of activity. We've seen a lot of… We've touched a lot of consumers; 22 million impressions that we've touched.

Keep going. They're telling me my show's over. You can keep going. I'm going to just hit a couple of other things.

A lot of social media work. Again, I can provide this for you later. We did a Times Square ad over the last holiday season last year, which gets millions and millions' worth of foot traffic, which was great. The last point is just, again, I think emphasizing this cross-industry communication.

We annually host a roundtable event, which we'll be doing in December of this year, where we invite in the US stakeholders and officials from many different agencies across government, private sector, non-profits, industry, with the goal of helping everyone understand what their respective viewpoint is. And every time we do this, we have amazing breakthroughs in the room of even, shockingly, government agencies realizing that they're not well-coordinated on this issue.

So I think it's all about having good information, good coordination, and good dialogue, and an understanding of the

evolving nature of these problems, so that, again, our companies stay in good standing and in front of the issue, and also are able to be helpful, because everyone in government, everyone in law enforcement, acknowledges that private industry can innovate and can be more effective in this space than they can.

So it's about finding that right balance of how we do that, but also maintain and protect our businesses, and become more effective, and save ourselves money, frankly, by being good in these spaces.

Thank you for inviting us. Thank you for listening and for your open mind and dialogue around this. Again, please do not hesitate to reach out and hopefully join the work that we've doing.

ALAN GROGAN: Thanks, Marjorie. The presentations that people are making here, they'll be posted on the website. They may not all be there now, but they will be by sometime later today.

Next, I'm going to turn it over to John Horton, who's also working on solving similar problems.

JOHN HORTON: Thank you very much, Alan, and for those of you I haven't met, John Horton with LegitScript. I look around the room, I see a lot of faces I do know, a lot of registrars and registries we do work with, so nice to see you. I only have about eight slides – eight or nine – so it's going to be very quick, go through them pretty quickly.

As Alan mentioned, LegitScript, just to introduce us, we're in Portland, Oregon, also here in Dublin, Ireland. We've got a staff of about 65, and what we're trying to do is provide intermediaries with information… Boy, that is not how that's supposed to look. That's okay.

ALAN GROGAN: [inaudible] PDF?

JOHN HORTON: No, that's fine. I think I can probably read through the text there. Why don't we just go ahead and go to the next slide since I've already been introduced?

As Marjorie indicated, why is this an issue that anybody should care about? It's unfortunately one of the highest risk sectors. There are some countries in which online prescription drug sales are not legal at all. They are legal in many other countries, but

when we look at it on a global scale, only about 3% of Internet pharmacies are operating legitimately.

To break that down a little bit further, I would say there's another 4-5% of those that we can't say are legal and legitimate, but the illegality doesn't rise to the level that we would notify a domain name registrar registry about it. Unfortunately, you've then got 90-92% of the domain names in the space that are doing basically three big, bad things wrong.

Number one, they're selling prescription drugs without a prescription. That is something that globally is not legal. I'm not aware of a single country in which that sort of thing's okay. Number two, the drugs are typically what's called unapproved for sale. That can include counterfeits, substandard, misbranded, and so forth. And then number three, they lack the legally required pharmacy licenses they're supposed to have. Our focus is on the domain names used to sell prescription drugs without a prescription. That's normally what we're sending to domain name registrars.

It's a patient safety issue. Some of the things we see – overdoses especially with controlled substances (the addictive drugs), when you have fake drugs, you can have a couple of different problems. There can be bad things in it, or even if it's just chalk or something like that, then you have a serious medical

condition — it could be cancer or AIDS or something — that is going untreated when the patient thinks it's being treated.

We do see deaths in this space, unfortunately, and prescription drug addiction. In my country, unfortunately, it's the number two drug problem, second only to marijuana. More than meth, heroin, cocaine, ecstasy, and all other drugs combined.

And this is an area where there is some degree of regulatory risk. Some law enforcement has looked to intermediaries in some cases if they're knowingly doing business with illegal Internet pharmacies. Go to the next slide.

We work either formally or informally with I would say most domain name registrars. We have formal agreements with some of you, and in other cases it's more informal, especially if we just need to reach out a couple of times a year. What we've tried to do is understand what do you need, what works for you, and we try to work within that framework.

And every registrar's a little bit different, but one of the things that we have often started out with is to say, "Let's take a look at your terms and conditions, your acceptable use practices." And in some cases some registrars have said, "We'd like to provide our registrants, our customers, with a little bit more clarity about what is allowed and what is prohibited." So for no charge – it's free – we've worked with registrars to help do that and

provide some clear language, but to the extent that your AUPs say you can't use domain names for illegal purposes is going to [stay] within that.

One of the big questions in this space obviously has been about content, and I think every registrar and registry in this room agrees you're not the content police, so let me address that head-on.

One of the ways I would say to think about that from our perspective is to bifurcate it a little bit. Nobody, I think, should expect a registrar/registry to screen every domain name. You can't do that. But there's a reactive way to approach it if you're provided with information – reliable information – establishing that the domain name is essentially being used as an instrumentality of crime.

Our suggestion would be take action on that. The standard we use is it really has to be solely or overwhelmingly the purpose of that domain name, not just something that's happening in sort of an ancillary way.

We stand by registrars throughout that process, even if the registrant comes back and says, "Hey, we're legitimate, what are you doing?" I'll describe our appeals process. If you get a rogue Internet pharmacy complaint from a third party, we'll review it for you. And there have been cases where we said, "We don't see

it here. We wouldn't necessarily be recommending you take action on it," or we do say, "Yeah, this looks like something that you might want to be aware of."

It's not just an automated process. I care about accuracy. Abuse reporters have to be accountable for the information they submit to registrars and registries. If we mess it up, that's on us. So here's the way that we handle that.

We have three analysts, at a minimum, that will have reviewed that domain name, and all had to agree that not only is it operating illegally in the sale of prescription drugs, but it rises to a certain level, that really most egregious level, which again, we're looking at chiefly the sale of prescription drugs without a prescription. We document that. Screenshots are documented, so if we need to go back, if you need us to go back and take a look, then we can do that. Again, we're focusing, if you want to go to the next screen, on that really highest level of legality.

Briefly, just an anatomy of a rogue Internet pharmacy. I'm not showing the domain name here because I don't want it to seem like I'm calling out a registrar.

This website is selling Xanax. This is a controlled substance. In other words, not only prescription drug, but also it is an addictive one. Every country in the world that I'm aware of,

alprazolam (the active ingredient) is a controlled substance prescription drug, if you want to click a little bit.

Here it's talking about an online consultation, which if you were to read through it — and I'll just race through this, and you can click again — it's essentially saying, "You don't have to see a doctor to get this drug." This, especially for this drug, is not going to be legal anywhere in the world.

And then the next click there. By saying it's shipping worldwide, a pharmacy license is required where you're shipping to. That just wouldn't be possible to have those pharmacy licenses. Let's go ahead and click through to the next slide.

This is what law enforcement seizures look like sometimes. Let's skip to the next slide.

I'm going to go forward to the Right to Appeal so I can wrap up here and talk about how we interact, how we try to protect registrant rights, if you want to go to the next slide.

One of the helpful things, I think, to think about is, again, any abuse notifier has the burden of evidence. When information is submitted to a registrar, that's an important way of protecting registrant rights. I think we can all agree on that.

Something I think a little bit different about the prescription drug and the online pharmacy space is once you establish that

some entity is selling prescription drugs, the burden shifts to a seller of prescription drugs to be able to produce a pharmacy license in the jurisdictions that they ship to.

The failsafe part of our process is if the registrant comes back and says, "What are you doing? I'm legitimate?" the first question is can you provide your pharmacy license where you're shipping to? And that's not an unfair requirement. That's something that exists everywhere around the world. We verify that. We've seen forged pharmacy licenses, and we work with you to get you that information.

We've never had a successful appeal, which means our anti-false positive rate is working. I'm going to leave the common questions to the end if you want to ask them so that we can save time and get to the other presenters. Thanks.

ALAN GROGAN: Thanks, John. Kristof Claesen?

KRISTOF CLAESEN: Good morning. My name is Kristof. I work for the Internet Watch Foundation. I'll be very brief, and I'll talk about a couple of aspects of our work.

The Internet Watch Foundation is the UK hotline combating online child sexual abuse material. We're an independent organization. We were set up almost 20 years ago by the online industry. We're mainly funded also by the online industry. We've got about 100 members. These include ISPs, hosting providers, filtering companies, registrars, social media platforms, and search engines as well.

We receive reports from the public about potential online child sexual abuse material, and our analysts can also go online and try to find these images themselves. We're encountering around 400 individual webpages depicting child abuse any given day. Over the year, we're talking about 30,000 to 50,000 — maybe more — webpages depicting child sexual abuse.

We've got a team of 12 analysts, so all the content that we see, it's a person assessing the content. They assess the content based on UK law, which is quite specific. Our analysts are also highly trained by law enforcement, and we've got a very extensive welfare package in place to make sure that they can deal with the content they see.

There is a gray area, of course, but we try to stay very much away from that area. We need to be certain it's a child, which can be difficult if it's a 17-year-old, because you can't tell if it's a

17- or a 19-year-old sometimes, and it needs to be under UK law sexual abuse. That reflects in the statistics as well.

Most of the webpages that we would assess as containing child abuse would depict images of children under the age of ten. So 80% of the webpages that depict those kind of images. And there is a percentage… Four percent depicts images of children under the age of two. That's 4% out of 30,000 or 40,000, so that's quite a significant number still.

I mentioned we work with the industry. There's not necessarily any legislation that says industry should do this. It's done for various reasons. Firstly, I think nobody wants to host child sexual abuse material on their networks. There's also a business reason. Nobody wants their customers to be exposed to this kind of material. There's a reputational risk if it turns out your company is showing or distributing or helping the distribution of these images. And we provide a number of services to the companies that they can use to protect their networks.

First of all, the best way to deal with this content is to remove it at source, so then the content is gone. In the UK, we can work with law enforcement, and we can issue a notice and take-down request to the hosting provider.

The good news is these requests are followed up on [inaudible]. Within 60 minutes after we sent the request, the content's gone.

The bad news is only 0.3% of the content we find is actually hosted in the UK. Most of the content is hosted abroad. We're talking mainly North America, Europe including Russia, and some hot spots as well.

We will pass on that intelligence to the relevant authorities in that country. Unfortunately, that process takes a lot longer, so we've got a number of other services that members can use. We've got URL lists.

This is a list of webpages that are depicting child abuse. It's URL-based, so it's at the most specific level possible, and ISPs can block their customers from accessing those webpages until the content is removed at source. We update that list twice every day, so it's very much up to date, and it contains probably around I'd say on average 1,500 URLs on any given day. But like I said, it's updated twice every day, so new ones are added and the old ones are removed.

We also have a hash list. We start hashing or taking digital fingerprints of images, which speeds up the process. Most of the images we see are duplicates, so if we have a [hash] fingerprint, it helps us speeding up. We don't have to reassess every image, and we can try to find those matches.

And also in this context we have a keyword list that can be used, for instance, by search engines, but also when people try to

register a domain with a certain keyword. That can be flagged to us, and we can have a look, and potentially some of the most obvious keywords, they cannot be or they should not be registered.

Now, there's always a problem. A lot of the websites that we see, the commercial ones, the big ones, they would have a random string of letters and numbers in their name. They wouldn't be as obvious as child abuse, and even if it's a keyword, there's always the potential that the content on the website is legal.

My colleague gave me the example, which I find very strange, it could be 13-year-old porn that could refer to child abuse, but it could also be referring to pornography that was produced in 2002, for instance, because that's 13-year-old pornography. It's very difficult, so that's where the hotline comes in, because our analysts can look at the images, can assess them, and make sure that the content is actually illegal.

The final thing I want to touch upon, because we're dealing with what people can and cannot see on the Internet, we're an independent body. We're a charity. We work with the industry on a voluntary basis, and we recognize that there are issues with what kind of responsibility does the charity have to decide what's illegal and what's not illegal, and we take that very seriously.

Two years ago, we had an independent human rights audit that looked at our framework that we've built around our processes in terms of accountability, transparency, the means to redress, and there have been a number of recommendations which we've implemented since.

Broadly speaking, the way we've structured our work and the safeguards that we have in place now are more than sufficient in terms of, like I said, transparency, accountability, redress, that our work can be considered as falling within the exceptions under the relevant human rights legislation. I think that's important for us.

It provides us with an element of protection, but also for members. When you talk about voluntary cooperation, you need to make sure that what you're doing is solid, that the intelligence you provide is correct, because otherwise the whole system fails.

I'm happy to answer any further questions about our work later on, and how we work with industry, but also have a look on our website. You can find us online at IWF.org.uk, or find me afterwards as well if you've got more specific questions. Thank you.

ALAN GROGAN: Thanks, Kristof. Toe Su Aung?

TOE SU AUNG: ICC BASCAP is a [CEO]-led initiative to fight counterfeits, by which I mean counterfeit goods – fake goods – which covers a range of products…which includes a range of products including soaps, shampoos, batteries. Whatever you can think of is included in this category.

Our members have had in particular a lot of focus on fighting the sale of counterfeits online. To be clear, I'm not talking about websites that sell a range of products, some of them real and some of them fake. I am talking about thousands and thousands of websites that exclusively deal with the sale of fake goods.

Before I came into this room, I spoke to two companies, and they said they were dealing at the time… One guy said he was dealing with something like 25,000 websites that he was monitoring for one brand, and if you have something like ten brands, that's 250,000 websites, and that was one company – or rather, two companies – with similar statistics. I can't say that all the companies have the same numbers, but we are talking large volumes.

We're not here to talk about how this can be regulated, but I think it's incumbent upon both brand owners and registrars to

get together and really exchange information on how this can be dealt with, because it's a pain for both sides, for brand owners and for registrars as well.

Today in particular I will speak about the EU MOU in 2011, which was entered into between leading e-commerce platforms and major brands in the field of all those goods that I just mentioned.

I need to acknowledge before I continue that lots of other associations were involved in this. BASCAP had a leading role, but other associations were involved – in particular, the European Brands Association (AIM) continues to play a key role in this.

The purpose of the MOU was to establish a code of practice in the sale of counterfeit goods over the Internet, and to enhance collaboration amongst its signatories so that everybody could respond effectively to the threat. The key aim was to instill trust in the marketplace. The MOU promoted trust in the online marketplace by promoting detailed measures against online sales, but also enhanced protection for consumers who unintentionally bought fakes as well.

I'll focus on two process issues and two key learnings from the whole process of negotiating and agreeing the MOU, which I hope will be useful for this audience.

Firstly, the actual process of discussion and negotiation towards signing the MOU, as well as the signing itself, really proved to be very useful steps in building a climate of mutual trust and confidence amongst the signatories. There were ups and downs in the relationship, but compared to the starting point, when parties were close to litigation –and in fact, some of them were in litigation – by the end, everybody had come a long way.

The structured dialogue really enabled the stakeholders to gain a better understanding of their respective concerns as well as technical and organizational and commercial limitations as well. So mutual trust and confidence were also unifying factors. However, to be honest, the open-ended discussions and the size of the group meant that this did rather drag on. It dragged on for almost two years of all-day monthly meetings of around 50 parties. Consensus was actually only reached when a handful of people had side meetings to [trade text] to get to something that the wider group could endorse or advise.

Drafting from scratch in a wide group and in a fishbowl simply failed to make progress. Apart from the logistics, the need for a small core group also came down to being able to talk about why particular wording or particular positions were acceptable.

Broadly speaking, while the bigger negotiation process was helpful, really we managed to make progress when there was a smaller group that was actually driving this.

The second key learning was the real usefulness of the facilitator. In this case, it was the European Commission that took up the role as facilitator of the dialogue. The commissioners at the time were considering legislating, and they were really keen to avoid legislating until absolutely necessary. So this really provided the impetus for drawing the parties together for a dialogue.

So the commission provided not only a convening function, but also logistical support, and they published summaries after each session. But they also ensured that the dialogue and the subsequent agreements were transparent and fully compliant with existing legal frameworks respecting fundamental rights. Without them, I think the parties would have taken much longer to get together and organize themselves, and certainly it would have taken much longer to actually reach a conclusion.

In conclusion, there are many learnings from the MOU that I think can be applicable to the whole situation of registrars and the sale of thousands of counterfeits brands on thousands of websites. I think the particular two concerns in terms of the registrar group is as the problem grows, the volume will get in

the way. I think we do have to work together to come to a solution that is practical.

Secondly, because consumers are involved, really we want to avoid the possibility of national governments enacting legislation, which is the situation in Europe at the time of the MOU negotiations. We really want to avoid piecemeal national legislation, which will really just further complicate our lives. Thank you.

ALAN GROGAN: Thanks, Toe Su. Tom?

TOM DAILEY: Good morning. I'm Tom Dailey. I'm the general counsel for Verizon's international business, and for many years I've actually played a role on behalf of Verizon in the public policy sector both internationally and domestically. I've dealt with many of the issues we've already heard about in terms of bad things that happen on the Internet. It's actually interesting for me to come back and hear the discussion this morning.

I'm here to talk about the voluntary program that Verizon played a key role in negotiating with other major ISPs in the United States, along with the content owners in the United States, roughly representing I'd say pretty close to all of the content

developed in the music space as well as the video and television space.

What we ended up with, as Alan mentioned earlier, was a program called – it's a voluntary program called the Center for Copyright Information. It's a notice-forwarding program essentially built around the notion that if we educate our customers – "our" being the ISPs in this equation – that we can help people understand copyright, help them understand that pirating material is not right and that there are implications to that, and ultimately try and move those customers over to a lawful means of acquiring the content that they're interested in.

It was interesting – and I want to talk a little bit about the process – because the program that we've had has been in place for a couple of years now. I was the chairman of the CCI for the first couple of years of its existence, taking it through the final negotiations, the stand-up, and then the launch. Then last year when I moved to London I turned the reins over to the general counsel of the recording industry, Steve Marks, who's now chairing the organization. So I can talk from a perspective not only as a participant, as an ISP – Verizon being one of the largest ISPs in the US – but also as a CCI board member and somebody who's really committed to getting the process working.

The slides that Alan put up are really… I was reading along some of the keys of these voluntary programs, and he's spot-on in the things that he listed, because many of those attributes are things that we encountered or dealt with or addressed in the course of the years – and I mean years – that it took us to get this program stood up.

If you go back about six years to 2009, that's when we actually started the negotiations of our program. We had a facilitator in the form of the attorney general of New York, Andrew Cuomo, who's now the governor of New York, and we sat down with a small group —I heard that mentioned — because I think you really need in something that is as controversial and contentious as content ownership, enforcing copyrights, and then the ISPs who are sort of on the receiving end a lot of this.

We have customers who may or may not be engaged in illegal activity, so in a sense we felt somewhat in the middle. We wanted to help, because we understood the problem, and we felt it was important to try and address piracy. The question is how do you do that in a way that balances the rights and interests of your customers with the rights and interests of the content creators and the content community. So we started with a small group.

We had a facilitator, and we had basically a very small, very senior level group of people from the music side and from the video and music/movie side. And we started working through what we felt from our side was not really the right starting approach, which was something not unlike the French "three strikes and you're out" program.

We didn't feel that that was really the right policy approach in the US, so we started from that foundation, and then just started working on something we felt would ultimately lead to a long-term viable solution that had the trust not only of both sides of the negotiation, but the trust of the public. Because at the end of the day, for those of you who were in the US when our program was announced, it was quite controversial. There was all kind of naysayers and skeptics in the media, in government, everywhere you look. If you hang out in Washington at all, you know how quickly those people can build a lot of views and opinions, many of which aren't right, but they come out.

So what we tried to do as we were building our program is figure out ways that we could address some of the key concerns that both sides had, one of which was privacy, because we knew that maintaining privacy for our customers and for everybody involved was essential to building trust in the program and acceptance of the program. Privacy was built into every aspect

of what we developed as we negotiated our memorandum of understanding (the MOU), which was ultimately signed in 2011.

And then, as we went forward building out the program, we had an appeal process that we developed that was also looking towards a trusted third party to help us build credibility and to build trust and acceptance amongst the larger community, so we went to the AAA, who does a lot of arbitration work, obviously, in the US. So they're the ones who handle appeals for customers who felt that they were wrongly notified, if you will.

So the program was really founded on a lot of principles that Alan brought up. It was based on how do we build trust, but the keys to success I think ultimately were the commitment level on both sides. We didn't see eye-to-eye at the beginning, but ultimately, after working together, both sides could ultimately develop a common set of commitments, a willingness to compromise. Nobody's going to get everything they want. But those are the keys: commitment, compromise, and then building trust for acceptance in the larger community.

ALAN GROGAN: Thanks, Tom. Roman Hüssy, and I apologize, but if we could go at a slightly faster pace, because there are people who would like to ask some questions, and we're going to run out of time if we don't do that.

ROMAN HÜSSY: I will try to make it very short. My name is Roman Hüssy, and I'm running Abuse.ch. Abuse.ch is a non-profit [project] that I basically run in my spare time. I have a day job, and in my spare time I try to work on Abuse.ch.

What Abuse.ch does is basically fighting cybercrime in terms of malware and botnets. We are talking about botnet infrastructure that is being used by hackers to control infected devices in the Internet, and about websites that have been registered for the exclusive purpose of distributing malware. That's the field I'm working on in my spare time.

I started to do that in I think 2007, and in this year I have started to [blog] about cyber threats first. I came up with websites that are meant to track specific botnets. Just for example, the [serious] botnets that some of you might know.

These projects are basically providing Internet participants, Internet users, the possibility to download some sort of block list that they can use to protect their own infrastructure and their own network from having infected computers within their network communicating with bad infrastructure in terms of [botnet] controllers.

I've started with this project, and during all these years there were some registries and registrars that got in touch with me and asked me what this is all about, and I've explained to them what I do. Some of the registries voluntarily started to block these domain names I'm listing on the website.

We usually don't talk about hijacked websites, because in my opinion you necessarily don't have to suspend a hijacked website because you can simply notify the webmaster of the particular website, and he will likely remove the malicious content.

Domains I'm talking about are purely registered for malicious purposes. So there is a hacker that's registered a domain name, and two hours later you will see it in a malware campaign hitting the Internet. That's the stuff I'm trying to take care of.

What I'm also doing , besides providing block lists for this kind of stuff, I also try to exchange, of course, threat intelligence data in terms of related to botnet and malware with other partners in the Internet across ISPs, registrars, registries, all the nonprofit projects such as the Shadowserver Foundation, who is also here today, and other block list providers. That's basically what I do.

ALAN GROGAN: Thank you. Nice segue. Benedict?

BENEDICT ADDIS: Hello. My name is Benedict Addis. I'm a member of your Security and Stability Advisory Committee, but I'm not here to talk to you as a member of the Security and Stability Advisory Committee. I'm here to introduce the Registrar of Last Resort, which is a nonprofit ICANN registrar that is set up to deal with the problems that Roman has introduced.

I'm an ex-law enforcement officer, and I notice there's nobody from law enforcement on this panel. That's one of the strange things about dealing with Internet you see in this field, that law enforcement comes to you, the community, as a supplicant as much as an authority. That's because law enforcement, outside of its own jurisdiction, only has the option to inform registries/registrars/hosting companies of malicious activity, and hope that people will act on their own terms and conditions to take that down.

Now, one of the things I've noticed is that everybody on this panel is in their own field committed to the problem in front of them. What's clearly emerging is there's a problem with scale here, where everybody is contacting bilaterally each provider, each organization that's represented here, and there is very little coordination. Law enforcement suffers the same problem.

Law enforcement officers suffer the same problem, because of the lack of regulation, the lack of due process in this field, often will reach out to registries/registrars directly, and often there'll be crossovers, so a lack of due process will emerge. So I'm here to talk about a new project which has been kicking around for a while and that I stupidly have volunteered to set up, which is an accredited ICANN registrar.

It's nonprofit. It's transparent, politically neutral, and accepts domains that have been used to attack the security and stability of the Internet. Unfortunately, I can't help most of my panelists, because we don't take reports on the basis of content, purely things like spam, phishing, the botnet problem that Roman's just illustrated. And the botnet problem is just massive.

We're talking, as some of you know — and I'm seeing some heads nod around the table — we're in a little bit of an arms' race with botnets at the moment. We have domain generation algorithms. That's the means by which an infected machine reaches back to its criminal controllers to either steal information or be instructed to go and attack someone. They generate perhaps, let's say, 1,000 domain names per week that are possibly called out to by each infected machine to receive their instructions.

The bad guys only register typically two or three of these, so we actually don't see them as a community, but each infected machine will churn through this list, and what this does is creates an arms' race. The defenders have to, every day or every week, register – obviously that's kind of expensive – or block thousands of domain names, and there are typically 40-50 families out there at any one time.

Meanwhile, the guys who are running these botnets only have to register two or three domains in order to gain and hold control of their network of zombies. And we're talking… A good-sized botnet is a million computers these days. The economic loss is horrendous.

The one that really got my goat when I was a law enforcement officer — I don't know if that's an expression that translates internationally — is Crypto Locker. Crypto Locker was a project by a hacker, a side project by all accounts, that locked people's computers and demanded a ransom to get those files back, a ransom of €300 a pop. This guy netted €30 million doing this project.

We've got the wrap-up. The registrar is designed to address this problem by coordinating between anybody that seeks to report malicious domains and the registries and registrars involved, so there's just one point of contact.

If we muck up, we have a redress program, completely transparent, and we will work with absolutely anyone. So I would encourage the registrars in this room, and the registries, to come and speak to me afterwards to discuss how that can work. Thank you very much.

ALAN GROGAN: Thank you. My colleague, Dave Piscitello.

DAVE PISCITELLO: Hi. Thank you very much, Alan. I am actually speaking today as a Steering Committee member of the Anti-Phishing Working Group and the Anti-Phishing Working Group for the European Union. I'll try to be fairly brief.

There are two programs that the Anti-Phishing Working Group provides that are of particular importance to this community. One is very similar to the block listing programs that my amazing colleagues Shadowserver and Abuse.ch provide. It's specifically a phishing stream. It's a data stream of phishing URLs.

The database is currently about 44 million URLs, and we recently began using the Facebook URL feed. Facebook was amazingly gracious in sharing this with us. Unfortunately, it's about two million URLs a month, so incorporating that into our systems has been a bit of a fire hose.

I don't have to talk to you about block lists except I'd just like to point out a timeframe that you have a sense of exactly what kind of remedies go where.

Normally, a phisher will begin by registering a domain. Within an hour, the phisher has hosted a site for the phishing attack to capture credentials, as an example, and then he'll launch his campaign by using spam (unsolicited mail). Normally within an hour – at most four – one of many of the block lists that we've already talked about will have added a URL that's been identified by a customer or what we call spam traps, and that mitigates the problem in some respects for people who are protected by block lists. But ultimately, as the gentleman at the end of the table said, getting the content down or having the domain stop resolving is the only remedy for protecting those people who don't have block lists.

With that, I'd like to just make mention of another program that APWG has that is sort of a remedy to some of these problems in terms of accelerating the suspension process. It's called the Accelerated Malicious Domain Suspension Program, and it's a voluntary program that can be implemented by any registrar or registry, and we currently have it experimentally implemented by about 20 parties. What we do is provide a vetted set of reporters – people who have high confidence and high trust and a good reputation, like the people here – a way to submit an

attestation and information directly to a registrar, and the registrar can process that much more quickly because he knows the party. There is a trusted third party who is vetting these and attesting to the credibility of these reports.

If anyone is interested in that program, I'd love to talk to you about it, especially some of the registrars who are here who are, I believe, already participating. I thank you for participating. I think it's a very, very good process, and it may help mitigate some of the problem here. Thank you.

ALAN GROGAN: Thanks, Dave. Frank Collin?

FRANK COLLIN: Thanks, Alan, and thanks for allowing us to be here. On behalf of the US Chamber of Commerce, which represents over three million businesses and associations internationally, we are very concerned with the problems of criminal activity online. We view voluntary initiatives as one tool in fighting this serious problem. We think this does not just affect our companies, but it's both a consumer safety issue as you heard earlier and also one that impacts individuals and companies, whether it's the downloading of malicious malware or if it's the theft of personal information.

From our standpoint, the Chamber sees this as a serious problem, and voluntary agreements are, again, one way to approach it. We have recently become supportive of one voluntary initiative that I'll highlight.

It's called the Trusted Accountability Group (or TAG), which was created by the Interactive Advertising Bureau and a number of other leading advertising agencies. The IAB, as those of you who may know it may know it, is involved in working on digital advertising issues. We see this as an issue that has to go to the core of people's trust in brands and brand integrity.

We certainly understand that one of the problems with some voluntary agreements is they're only effective as their terms and their level of participation. For voluntary agreements to be effective, people really must buy in. They must really participate in the program, be committed to them.

There are many times when we see voluntary agreements that are well thought of, and they're good ideas but ultimately they're not really solving the problem. What happens then is the risk of government intrusion.

One of the concerns we have at the Chamber, we're not supportive of a lot of government regulation. We believe that there should be some and at an appropriate level, but business

should also be able to operate, and certainly in the Internet, in the fashion that suits industry best and consumers best.

From our standpoint, we think that if you continue to see criminal activity in the online space, and voluntary agreements are not effectively addressing the problem, you have the real risk of government stepping in. We certainly think this is a problem, as Toe Su mentioned earlier, that exists not only in the EU, but also in the United States.

Also, industry benefits from certainty in the environment in which it's operating. When you have uncertainty for industry and uncertainty for consumers, you create additional risks.

All companies, regardless of the type that they are, depend on their brand. They depend on consumer confidence, and when you expose your customers to criminal activity in the online environment, you certainly create additional risks for your brand.

From our standpoint, we represent companies that are the leading tech companies, leading manufacturing companies, leading entertainment companies, and leading pharmaceutical companies. All of them share the same concern. They all do business online, and they all want to make sure that they have an opportunity to operate in a space that's safe and secure.

The last thing I'd mention is certainly we understand that there are scales here in the types of crime that we see occurring in the online environment. People are at risk of the dangerous medicines Sean and Marjorie talked about. Certainly that's a higher level than somebody who might be purchasing a fake product, but you also have to remember that fake products, I think, as Toe Su well knows, may be produced by child labor. There may be other criminal enterprises associated with the production of these types of materials. These criminal enterprises are not simply engaged typically in one type of criminal activity, so to look at this as something that's simply because it's a certain type of crime that does not seem as serious in the online space we believe is being a little bit narrow-minded.

We would urge everyone to take a look at those voluntary agreements that are effective. We think that one of the important things is also if there are existing other methods in place to try to deal with problems, that folks live up to their obligations.

We appreciate ICANN's attention to these issues. We certainly do believe, as I said before, that voluntary agreements are part of the issues in terms of solving the problem, but we also would hope that whether it's contractual compliance or it's other types of effective ways to solve some of the problem our companies

are dealing with, that everyone takes the situation seriously and actually participates in trying to solve the problem.

So, Alan, thank you very much for your opportunity to speak today, and happy to answer any questions.

ALAN GROGAN: Thank you, Frank. I did get a request from somebody to provide contact information for all the panelists, so I will make sure that's posted online so people know how to get in touch with them later.

Bertrand, can you spend about five minutes talking about the Internet Jurisdiction Project? I apologize; I think we're going to run out of time for questions, but I'll d a quick wrap-up after Bertrand.

BERTRAND DE LA CHAPELLE: Very briefly — and hello, everybody — the problem we're confronted with is basically a problem of the [patchwork] of jurisdictions and [attention]. That is, existing with the fact that the Internet by definition and by value is across borders.

The problem is in this context, apart from the issues that have been mentioned so far, there's a domain that is very contentious, which is content, that is legal in one country and

illegal in another one. Typically we're talking about hate speech, incitation to violence, and all those things.

There is no international framework that solves this problem at the moment, and there's no likelihood that there will be a harmonization [on substance], nor should there be a harmonization [on substance]. The norms that order potential restrictions on free speech and freedom of expression are different from country to country, and deeply ingrained in the identity of those countries.

The key challenge is that at the moment when there is a problem, there is no international framework. The mutual legal assistance treaties do not function in those regards.

Without getting into too much detail, the reality is that today there is an increasing number of direct requests for domain seizures or content takedown that are being addressed directly by law enforcement or public authorities in one country to intermediaries in another country. This can be major Internet platforms, like Facebook, Google, and others, or it can be DNSO operators.

This raises a large number of problems, and among the other things, it forces private actors to make decisions that are [quasi-judiciary], and that are weighing principles regarding freedom of expression, liberty, and all those kinds of human rights, which is

not very pleasant as a situation and raises concerns more generally in terms of procedure.

Without delving too much into content takedown, I want to address the issue of using the DNS as a level and as a layer to address issues related to content. Here there is a misunderstanding, and a deep misunderstanding, that most of you must be aware of, which is that it is very tempting when there is a content that is illegal in one country to go to the DNSO operator and say, "Okay, flip the switch." Because, of course, that's a very nice switchboard. The problem is the following.

There is a need to put forward a principle and to affirm the notion that the DNS is a global, neutral layer, and that fundamentally any action that works at that level has a global impact. Therefore, it should be used mostly for issues that have a global impact and that, for instance, either abuse or harm the DNS itself.

That includes phishing, botnet, malware, and all those things. I think most of you have regulations in your terms of service that concern this.

The question related to content has actually been said in [inaudible] by almost everybody. When it is about content, using the DNS layer is legitimate if (and probably only if) the entirely of

the domain is being used for an activity that is sufficiently globally considered as unacceptable.

I think this permeates all the comments, and I think it is a sort of message that is a completely different message from the location of the operator, the incorporation in one country or another. This is a general principle.

That being said, what we're doing is we've been facilitating a dialogue among more than 100 actors in the last four years from governments, civil society, major Internet platforms, DNS operators, and international organizations including OECD, Council of Europe, Interpol, Europol, European Commission, and others.

The goal is to develop a transitional due process framework for those [transporter] requests for domain seizures, content takedown, and access to user identification. This framework has now reached the stage where there is a general architecture of two pillars for submission of requests and handling of requests.

The submission of request is organized around templates and standard request formats, and handling of requests is being structured around the documentation of what are the current best practices within Internet platforms for DNS operators and common criteria.

I'll stop here. The general objective is to have a mechanism and a system that ensures what we call legal interoperability protocol, so that basically the actors who submit requests and the ones who receive requests have a common understanding. Anybody who's interested in knowing more, I'm very keen on paper, so in this environment, if you want any explanation or description in more detail of what the architecture is, you're welcome. Some of the actors in this room are actively engaged in the process, and we will enlarge the number of participants in the coming year.

ALAN GROGAN: Thank you. I want to thank all the panelists. We're up against the end of the session, so if you want to reach out to any of the panelists, I'm sure they'll be around and be happy to talk to you.

In terms of next steps arising out of this, I think purely voluntary actions — obviously contract parties are welcome to take off on their own at any time reliance on malware and child abuse image block lists and those kinds of things.

The other potential is that parties could decide to get together to negotiate a framework for solving some of these problems. They could do that on their own initiative or through facilitation by some trusted mediator.

I don't think that it's appropriate for ICANN to be that trusted mediator, because I think that's outside the scope of our mission and remit, but a successful outcome, if the parties decided to engage in that to address any or all of these problems, I think would be a framework that's negotiated and implemented outside of ICANN for voluntary market-driven self-regulation. I thank you all for your time. Feel free to reach out to me or any of the panelists.

UNIDENTIFIED MALE: [inaudible]

ALAN GROGAN: Thank you.

[END OF TRANSCRIPTION]