HYDERABAD – DNS and Content Regulation NCUC Group
Sunday, November 06, 2016 – 17:00 to 18:30 IST
ICANN57 | Hyderabad, India

RAFIK DAMMAK: Okay. Thanks, everyone for joining this high-interest session -- I mean, topic session. So we are going to talk about DNS and content regulation. We tried for this session to really bring the different and the diverse point of view regarding the content regulation within the ICANN context. And as you may see, you see we have several speakers on the panel. However, we will try to be brief in the term of intervention.

Just maybe to give the context here is that the topic came from -- just maybe to present myself first, Rafik Dammak, I'm the NCUC chair. The topic came from one of our members, the Electronic Frontier Foundation. And they suggest maybe we can have cross-community discussion about content regulation to include everyone from the business side, from law enforcement, from the contracted party, and so on.

And for that, I want to give the floor for Mitch in just one, two minute, to try to give really the context and set the scene.

MITCH STOLTZ: Thank you, Rafik. This is Mitch Stoltz. We proposed this session to discuss a very simple principle, whether ICANN and more broadly the Domain Name System and its participants, should be used to regulate Internet content. I'm here to say and I think many people believe the answer is a firm no.

The Internet is a revolutionary system for open communication in large part because it's decentralized. That makes it hard for any one person or group to control speech or to block speech they find undesirable. But, of course, the Internet does have its chokepoints and its points of control and the Domain Name System is one of those.

Chokepoints create a strong temptation to many different interests to use -- to regulate speech, all kinds of purposes, both noble purposes and less noble purposes.

The new ICANN bylaws contain a strong statement of principle that the content of websites and Internet services is beyond ICANN's remit. But there are also several loopholes and qualifications to that statement written in the new bylaws making this still a live issue.

Beyond the formal ICANN mechanisms itself, there are -- have been a number of initiatives in the past year or two to increase the use of domain name suspension or threat of suspension as a means of regulating content along several lines, including

copyright, professional licensing, regulation of certain product sales, particularly pharmaceuticals. And there have also been some attempts to bring those outside -- I believe these are attempts to bring these outside arrangements among the contracted parties and other outside organizations who have special interests in these areas under the ICANN umbrella, sort of use the imprimatur, if not the bottom-up multistakeholder processes of ICANN, to give some legitimacy to this concept.

The concern here at which I think is shared by many is if this line is breached, the line between regulation and management of names and the regulation of Internet content, I'm not sure where there is another firm line that can be drawn. And that's something I wanted to -- hoping that we could discuss at this session, is where we go from there beyond copyright, beyond professional licensing, and so on. Is there another line to be drawn, or is that a -- going in a direction of broad -- of, I guess, sort of broad speech licensing regimes, a place we should not go? Thanks.

RAFIK DAMMAK: Thanks, Mitch, for this.

So here we gave one quick overview of what we are trying to achieve. And then I would like to pass to Allen Grogan who will introduce, I think, the Registry and Registrar Agreement so that

give us some framing for the discussion, one of the initial framing.

Can we please move to the other PowerPoint?

ALLEN GROGAN: Can you advance to the next slide, please? All right. Not the right slide. Anyway, so I think somewhere in the slide deck there's a presentation on ICANN's mission and bylaws and also key provisions in contracts with registrars and registries primarily from the 2013 RAA. I'm not going to spend a lot of time on this. Rafik saw the slides and panicked, and I assured him I would get through this in about three minutes. So all I want to say is as Mitch already mentioned, under the new mission and bylaws, there's an explicit prohibition on ICANN acting outside its mission. And I will leave it to you to review the mission because it's lengthy, and we don't have time to go through it.

But oversimplified, it's largely technical in nature. It relates to the coordination and allocation of names in the DNS, facilitating and coordinating the operation of the DNS root server system, coordinating the allocation and assignment of the top level of Internet protocol numbers and autonomous system numbers and so forth.

There is an explicit prohibition on ICANN's regulation of services that use the Internet's unique identifiers or the content those services carrier provide and explicit acknowledgment that ICANN is not a regulator.

However, there is a grandfather clause, if you can go to the next slide, that essentially says agreements entered into prior to October 1st of 2016 or agreements in the same form or substantially the same form as those agreements and any renewals of those agreements, ICANN can enforce and contractual compliance is responsible for enforcing those contract provisions. And I have set forth in the slides for you to look at later -- I'm not going to go through them in detail now -- but recognize that in the dialogue with the community and in the dialogue we're having on the panel today, whatever someone wants ICANN to do in terms of combating abuse either needs to be within the scope of ICANN's mission or it needs to constitute a breach of a specific contractual provision that fits within these grandfather clauses. We can't just make up authority to regulate abuse.

And maybe if it's useful, we can refer back to these slides if and when issues arise in these discussions. Otherwise, I'll leave it to you to review them at your leisure. Thanks.

RAFIK DAMMAK: Okay. Thanks, Allen.

I think Steve, Steve DelBianco, want to maybe add something here regarding the new bylaws.

STEVE DelBIANCO: Thank you, Rafik.

As one of the members of the cross-community working group on Work Stream 1, I feel as if I've done, what, four years of law school study under the tutelage of Becky Burr and all the other attorneys that were involved in that, including the outside counsel. It still doesn't make me a lawyer.

But I can tell you this, Allen's description of it makes it seem as if it was only the grandfather clause that creates the opportunity to have things like safeguards present in the contracts. Well, Becky Burr and the CCWG legal advisors said the opposite. They believe that the safeguards or public interest commitments entered into the contracts were not the same thing as regulation of conduct -- content. And they wouldn't have been prevented as if they were regulation of content. But for avoidance of doubt, a new phrase I learned from the lawyers in CCWG, for avoidance of doubt was added so that it was very clear to anybody scrutinizing the transition that ICANN was not about to blow up contracts with several hundred new gTLD registries;

that those contracts would be enforceable throughout their life and renewal. And the development of new contracts, however, would go through a different lens, a different process, because one of the most important parts of the mission statement is that future agreements and policy have to fit within a bottom-up multistakeholder-driven process. And that means that opportunities for late-in-the-game or even last-minute clauses coming down from the GAC or anyone are going to be significantly impaired. Instead, we'll try to really work through our bottom-up process to get there.

And I think that we also clarified, as Allen just said, that the creative -- creation of new contracts, including public interest commitments, may be in service of ICANN's mission. We clarified that. We clarified that enforcing policies in contracts in service of its mission is entirely within ICANN's remit as well.

So I think that it's -- it's a mistake to believe that these public interest commitments were somehow an anomaly. I think the process by which they came down from above is not likely to happen again. But they are not per se the regulation of content and, therefore, you can't say that they are somehow an exception.

We may well find ICANN in a situation where ICANN contract parties undertake commitments to the registrants, to the end

users, to governments, businesses, and others. And those commitments, if they're in the contract, are going to be enforceable by ICANN. Thank you.

ALLEN GROGAN: Let me just quickly respond because if there were any misunderstanding of what I say, I think in general I agree with what you said. The PICs are part of the contract. So when you look at the contracts, those are absolutely enforceable. They are embodied in the language of the contracts, and those are enforceable against the parties the same as any other contract provision. And that was the purpose of the grandfather clause.

My point was simply when you are looking at what we can do to combat abuse, it either needs to be in the contract, which includes the PICs, or it needs to be in the mission. Those are kind of the two possibilities in the new framework. It's got to be part of the mission or it has to be part of contract provisions that were grandfathered in and we are explicitly allowed to enforce.

STEVE DelBIANCO: And also consensus policies. If we develop consensus policies in a bottom-up way, those consensus policies are enforceable by the same way.

RAFIK DAMMAK: Thanks for this clarification. So I think now we kind of set the scene for the second part of the discussion.

We are going to -- through several -- sorry. We tried to think about possible scenarios that what may lead to the content regulation context. And as you may see on the screen, so we have different cases.

After that, we will try to go through several of the questions to get some feedback and intervention here.

So I won't try to go through all the scenario, but as you see, we have really different cases between that content that can violate copyright law or maybe some content that may violate government law against hate speech or political critique and so on.

Saying that, so we will try to respond to the first question or discussion question, which is the domain name infrastructure sometimes is used to enforce laws or policy governing fair content of website and other Internet resources. How does enforcement through domain name suspension compare with other avenue of enforcements such as court orders to the website or owner or host or enforcement through financial system and advertising network?

For this, maybe I would like to start first with the registrar and maybe start with Michele.

MICHELE NEYLON: Thanks. Thanks, Rafik. Michele Neylon for the record or whatever.

The question, I suppose, is a bit -- is a bit nuanced. There are policies that all ICANN-accredited registrars have to abide by. So if, for example, a domain name is found to be problematic due to -- in a UDRP or a URS, then obviously under the contract we have no choice but to follow that. That's within that remit and scope.

However, I think when it gets outside of something as clear-cut as that, speaking as a hosting provider, I don't want to be in that position of having to make an arbitrary decision. But I can make an arbitrary decision, if I have to. Ultimately, you choose to host a website, to register a domain name with a private company. You can choose to register, host it with any private company. If you choose to register and do it through ourselves, you are bound by our terms of service. And if we find you to be in violation of those, we can, we will suspend you.

Now, the thing, of course, is there's a big difference between a domain name that is being set up solely for the purpose of

infringement or a domain name/website that has been compromised. There's a massive difference there.

For example, for us, we get abuse reports about websites that are being used for phishing attacks, distribution of malware, and all sorts of other charming nefarious activities. If it's due to a compromise, than we can either shut down the website only but leave the email and other services running. But if we're -- we're expected to take down the domain completely, we can kill off perfectly legitimate services. It's -- and it's not a simple question. Because ultimately as an Irish company, we are bound by Irish law. I'm not going to act on a court order from the court here in Hyderabad.

Now, if the court in Hyderabad, for example, was to send us something and I could actually understand what they were talking about, we might investigate it obviously. But I can't act outside the scope of what I'm allowed to do. I don't know if that's of any help to you.

RAFIK DAMMAK: Thanks, Michele. Maybe -- let's get maybe the perspective from the guys like trademark and ask Steve Metalitz what he may think about this.

STEVE METALITZ: Yes. Thank you. This is Steve Metalitz. I think Michele made a very important point which Mitch's first presentation kind of blurred. And I think it's kind of important to maintain this distinction. There are things that ICANN is doing to enforce the types of laws and policies that we may be talking about here, and then there are things that ICANN-accredited registrars or ICANN, you know, registries, gTLD registries, choose to do in deciding who their -- what their terms of service are going to be.

There's a big difference there. We've had many discussions here within ICANN over the last year or so about particular provisions of the -- and I'm sure they're in Allen's slide deck somewhere -- of the Registrar Accreditation Agreement, two or three provisions that are relevant, and some provisions of the new gTLD agreement, in particular the public interest commitments. There are a range of views on what those provisions require, what they require ICANN to do or what they require the companies subject to those contracts to do.

But that's quite -- and I'm sure that discussion is going to continue. But I don't think that's really what we're here to talk about. If we look at this handout about shadow regulation, that's not what this is about. It's not about ICANN enforcing anything. It's about something that we're told is taking place under the ICANN umbrella. I have never actually seen the ICANN umbrella. I'm not sure what it would protect us against.

But I see these as activities of private companies who are choosing who they want to do business with and it's quite standard to have a term of service that you can't use their service for illegal purposes or to commit crimes.

So, for example, the reference in this question to financial systems, advertising networks, payment providers have very similar terms of service in many of their contracts. Advertising networks may have the same types of provisions in their terms of service.

And there the issue is: Is it a positive or a negative for these voluntary agreements to be reached where the people that are providing important services in the Internet environment take reasonable steps to try to prevent their services from being used for illegal activities. And that's -- I think that's an extremely important part. It's not going to solve every problem by any means. But it's an extremely important part of efforts to try to deal with serious problems of abusive activities that are taking place on the Internet. And I think to characterize these as regulation of content is really quite misleading. This isn't about taking anybody's content. The content is still there. The issue is about providing an easy path for that content that may be in violation -- or it leads to conduct such as is explained in some of the examples on the previous slide that may be in violation of law.

So, again, I think the voluntary agreements and voluntary policies that registrars and registries, among others, among many others, are following is a really important ingredient in providing a safer, better Internet for consumers around the world. And I think it's something that we should be encouraging and not discouraging.

RAFIK DAMMAK: Okay. Steve, I think this looks like directed to Mitch. He may want to respond to this.

MITCH STOLTZ: Yeah. Thank you. A few things about that. Starting -- starting with terms of service -- and I mentioned this to the board in this morning's session with the noncommercial stakeholder group -- every business does set the terms under which it does business and it sets those terms to protect itself and to characterize its business and, in a sense, to market its business to whatever customer base it chooses. Every business does this.

Having terms of service does not mean that third parties, strangers to that contract, gain any rights.

And so the notion that, for example, copyright holders or anyone who claims to be aggrieved by a violation of some law or policy, has standing under a registrar's terms of service to force some

enforcement. Again, really what we're talking about is domain name suspension or the threat of suspension. Yet that turns that terms of service into a law, for all practical purposes. No longer a commercial contract, but a law that's enforceable by anyone and binding on everyone. It's a very different sort of -- sort of scenario.

Then this notion of voluntary agreements. Again, every registrar, every contracted party, every business really chooses the terms under which it does business. It is important that there is diversity, that there is choice, and that there is competition among those terms. Especially when we're talking about things that -- where the contracted parties have no legal responsibility.

A contracted party, under the law of every country I'm aware of, is under no legal obligation to enforce copyrights or most other laws. There are -- there are going to be some -- there are going to be some exceptions. You'll have -- Michele mentioned. But there is no legal obligation, because the contracted parties cannot be liable for the copyright infringement of a third party except under very narrow circumstances. Again, under the law of every country I'm aware of.

These are -- these are choices, but if every contracted party is making the same choices, whether because they were imposed

by ICANN or whether because they're set out as so-called best practices, then there is no choice and then the set of practices really coming from particular special interests -- and I'm talking about the entertainment industry, particular law enforcement interests, particular professional and regulatory bodies -- you know, becomes a sort of global law, which is a dangerous proposition.

There is no global definition of abusive activities, and it's very dangerous to bring things under such a broad brush and very dangerous to say that there is a single set of policies for a safer Internet, especially if safety is broadened to include things like copyright.

RAFIK DAMMAK: Okay. Thanks, Mitch.

I see many hands rising, starting with Michele and Liz, Jon, and then Robin. Please be brief.

MICHELE NEYLON: I'll try.

For the -- for one of the first times in the history of my attendance at an ICANN meeting, I find myself in strong agreement with Steve, which is --

[Laughter]

MICHELE NEYLON: -- which is not normal at all.

[Applause]

MICHELE NEYLON: I mean, look, ultimately, Mitch, with no disrespect, I think you are trying to build a case for some kind of black helicopter-type scenario where we're all colluding to -- to take away some rights from people when we're actually not.

Now, if you have specific cases or specific issues, please speak to them because I'm listening to you and you're talking about this stuff at a very high -- high kind of philosophical level and it -- it sounds wonderful and you've got lots of nice little words in there, but I don't see something concrete.

Saying that -- that registrars are somehow creating some kind of monopoly in terms of our terms of service is ridiculous because we compete against each other actively. I get out of bed in the morning and I check to see what my -- what my competitors are doing in terms of pricing and I lose domain names to them over a couple of cents. There is a massive amount of competition in the marketplace. It's not going anywhere. But I don't -- this --

I'm just trying to understand what it is you're pushing -- pushing and I don't understand it. Because if you're saying that I should have terms of service that allow people to -- to break the law or to disrupt the DNS or to create an unstable Internet, then I -- we're never going to agree on this. If it's something -- something else, please be specific.

RAFIK DAMMAK: Okay. Thanks, Michele.

Okay. We have Allen and then Liz.

ALLEN GROGAN: Yeah. Just real quickly, without -- without addressing the sort of philosophical questions that have been raised, from ICANN's point of view if there are agreements that are entered into between two private parties, one of whom happens to be a registry or a registrar, I don't see that ICANN has any role to play in deciding what kinds of agreements those parties can enter into. That clearly is outside the scope of our mission and remit. We can't compel a registrar or a registry to even tell us what those agreements are. They're free to enter into whatever contracts they want to enter into. To the extent that they become embodied in the contracts as PICs, that -- you know, that may be a different question, or to the extent that the

agreements violate those contracts or violate consensus policies, that may be a different question. But if -- if a registrar or registry decides to enter into an agreement to trust the MPAA or law enforcement or anyone else in deciding what actions to take, I think they're -- they're free to do that and it would be far beyond the scope of ICANN's power or authority to do anything about that.

LIZ FINBERG: Liz Finberg, PIR. So I will say I'm also in rare agreement with Steve, and I would tell you, Mitch, that, again, to echo Michele's point, the notion that somehow everybody is going to start doing the same thing and we're going to somehow create law is really very far from the truth. I think even among this panel there's a -- there's a range of approaches of those who would say, you know, "If you want us to disable a Web site, get a court order," others who would participate and who do participate in trusted notifier programs, and then somewhere in the middle, which is where we are, in trying to set up an ADR procedure whereby in our case the registry is not enforcing a law, it is entrusting it to an alternative dispute mechanism which will guarantee due process, rights of appeal, and which, by the way, would require a higher standard for suspending a domain name than what a federal court would require.

So I mean, the point is, there's a range of -- of approaches and it's -- in no way is this a concerted effort by the industry to suddenly become lawmakers.

The other thing that I wanted to ask -- and I know there are other people in the queue, but I'm curious to see -- or curious to hear your rationale for why enforcing or having, you know, terms of service somehow creates law. It's -- it's exactly the opposite, in my view.

As you said, every -- every company -- and, you know, companies within the DNS and this industry are no different -- have a right to set their terms of service, and so I don't see that as creating law. It's very much a private, you know, company-by-company decision. Thanks.

RAFIK DAMMAK: Okay. Thanks Liz. Just to assure those on my left, we are going to --

[Laughter]

RAFIK DAMMAK: So we have Robin and then we go to Steve DelBianco, Jon, Steve Metalitz, and Thomas Rickert.

Yes, Robin.

ROBIN GROSS: Thank you. This is Robin Gross, for the record.

Well, from the perspective of registrants, there's a number of concerns regarding taking down Web sites based merely on allegations and without a -- without any kind of a court order. And of course one of the biggest problems is the lack of due process. Courts are in -- are designed to ensure fairness. They're designed to ensure due process. When you're going to deprive somebody of their right to speak on the Internet through -- through a domain name, there are mechanisms in place that make sure these appropriate concerns are accounted for.

You don't get that when -- when you've got a contracted party just taking down a domain name based on an allegation.

There's no expertise, really, no legal expertise that can be relied upon within the -- the various contracted parties. I mean, laws are going to be different in different jurisdictions and it's frankly too much to ask for contracted parties to be aware of all the differences in laws and all the nuances and to have to make these kinds of legal determinations, and that's why it's appropriate that they should have to go through an appropriate process and get a court order.

They -- they've got an incentive to err on the side of taking things down. Contracted parties they don't want to be held contributorily liable or liable for any kind of actions that are

done by their customers, so there's an incentive there to really err on the site of censorship and err on the side of taking down information that doesn't need to be there. So it ends up being overly broad, too, when you're taking down entire domain names or entire Web sites based upon maybe a single -- a single thing that's in dispute here.

And, you know, if you want examples, anyone -- anyone could just go to the chillingeffects.org Web site where there are bogus takedown claims that are accumulated and posted by the thousands, and so, you know, it's not like this is really some kind of abstract pie-in-the-sky scenario. I mean, I'm sensing a bit of defensiveness from the contracted parties and I get that, but these are real situations and this happens all the time and all you need to do is go to the chillingeffects.org Web site and see all kinds of examples of the kinds of bogus claims that are made and then contracted parties feel pressure and have the incentive to remove that information without any kind of appropriate process. Thanks.

RAFIK DAMMAK: Thanks, Robin. Jon?

JON NEVETT: Sure. Thanks, Rafik. Jon Nevett from Donuts.

Everybody has been piling on Mitch except for Robin, I guess, so let me start with: I agree with Mitch in the first thing he said, which is, you know, we believe in an open Internet, open TLDs. We don't think there should be ICANN regulation of content. So we're aligned on that.

For example, we are the registry operator for .DOCTOR. We went through a huge fight with -- in the ICANN process to make sure that was open. Many people wanted that closed to just licensed medical practitioners and preventing people like Steve Crocker to get dns.doctor or someone who is a lawyer getting juris.doctor, and I -- we fought that alongside with people in the NCUC and NCSG and won, because it was the right decision and the right thing to do, that --

We shouldn't have ex ante enforcement. We shouldn't prevent people from speaking.

However, we believe strongly in ex post enforcement of requirements and ex post regulation.

So we said, "Well, if someone's going to hold themselves out as a licensed medical practitioner in .DOCTOR and they are not one, after being challenged, then that should be an issue and we should do some kind of takedown or suspension."

So that's the philosophy we approached this. And you could extend that to other types of misuse on the Internet.

For example, child imagery abuse. You know, if we get a complaint through a trusted notifier relationship with an entity like NCMEC in the U.S. or IWF in the U.K. and they say, "There's child imagery abuse on this site," we're going to take it down. We're not going to wait for the victim to go get a court order. I'm sorry. That's just -- you know, we're a private company. Our reputation is on the line with our names. We want to keep a clean healthy space. And if we have a -- we have someone that's an expert in this industry that we have a relationship with saying there is child imagery abuse going on in a name, we're not going to make that victim go get a court order. We'll take it down. Now, if the registrant wants to go get a court order after and say what we did was inappropriate, that's fine. We'll obviously follow the court order.

The same is true with other forms of abuse, be it phishing with the antiphishing working group, or, you know, other misuse or harms that -- that we approach and we see every day.

So real-life example. We had a complaint that someone registered rape dot one of our TLDs, and it was a how-to guide. Talk about a horrific Web site. And, you know, we got a complaint. I'm not going to wait till someone goes and gets a

court order. This is -- we're a private company and we -- we agreed to suspend that name immediately and that's fine, and there was no due process.

And I'm cool with that because that was the right thing to do.

And, you know, there are other cases where the harm may not be as great as that case, where -- in, let's say, a copyright abuse case where we get a notification of some kind of illicit, illegal download of copyright material. You know, we give the opportunity for the registrants to respond. We'll look at that.

You know, this trusted relationship we have with the MPAA, for example, has been criticized by Mitch and others. Over nine months, we've received 12. 12 referrals. This is the bad of the bad. You know, these are cases -- most of them were subject to court orders for different domain names, same exact site. So do we make the -- the movie studio go back to the court and get that -- that same name for the same site added or do we do the right thing by following that same court order for our name? And we decided we'll do the right thing and do that. And, yes, it's our view that it's the right thing but it's -- we're the registry operator. Just like a restaurant could determine that they don't want people with shorts and flip-flops in the restaurant, you know, we don't want illegal behavior, and if they want to move somewhere else, let them move somewhere else. That's fine. If

you want to have child imagery abuse on a different network, a different registry operator's name, you know, go -- go for it and hopefully they'll do the right thing, but I don't have a problem with that.

And so when we're -- we're here, we're looking at this stuff, we're not doing it to protect ourselves necessarily. We're also doing it to protect consumers and folks who are harmed by this misuse.

So the -- and to Robin's point, our incentive is not to take down our customers' names, believe it or not. We want our customers to be happy. We don't want to not get renewals. You know, we're a business so we're -- we're -- our incentive is to make sure that we're really sure if we take something down that it's really misuse and abuse.

And we're certainly not making law, Mitch. You know, I -- I don't -- don't profess to be an lawmaker or someone who wants to be a lawmaker, but that's not what we're doing with these relationships. What we're doing is enforcing our code of conduct, our acceptable use policies, which thousands of businesses do both on line and off line, and I'll defer to the next person. Thank you.

RAFIK DAMMAK: Okay. Thanks, Jon. So we'll try to get intervention from the rest of the speakers and also we'll try to move to the next question because time is going.

Steve Metalitz? Yes.

STEVE METALITZ: Thank you. I think just briefly, what we've just heard from the last several interventions is illustrative of the variety of different approaches that different companies are trying in different -- in different settings. Whether it's, you know, an ADR type approach, as PIR is talking about, or the trusted notifier approach that Donuts has implemented, those are two different ways of dealing with this and they may be -- may have varying degrees of effectiveness, but I think the idea of encouraging these types of voluntary approaches also includes --

The distinction that -- that Jon made I think is very important made between ex ante and ex post enforcement. Some registries have an ex ante policy and say "You can only" -- you know, there were applications for new TLDs that said "You're going to have to show your copyright ownership before you can register in a particular TLD that's clearly targeted to copyrighted material." Others took the Donuts style -- Donuts style approach and said anyone can register. But then once -- you know, but once information becomes available that it's being used for

illegal -- clearly illegal purposes -- and I would encourage people to look at some of the information that Donuts has made available about how their system is operated because I think it helps to dispel some myths about, you know, taking down an entire site because there's one piece of copyrighted -- you know, of copyright infringement on it. That's not what these cases are about. No one is depriving anyone of their right to speak on the Internet. As Jon pointed out, they have other alternatives and other places they can go to speak. And the chillingeffects.org site has nothing to do with this because that is about taking down particular items on particular Web sites under the laws of a particular country, the Digital Millennium Copyright Act in the U.S. So it really doesn't pertain to the -- the situations that we're talking about here.

RAFIK DAMMAK: Okay. Thanks, Steve. Steve DelBianco?

STEVE DelBIANCO: Thanks, Rafik. This is called a high-interest topic and I think I know why, because we -- we would have to be high to believe --

[Laughter]

STEVE DelBIANCO: -- that if a registry or registrar took action based on a complaint, that that is the same thing as making law or creating new rights.

The programs we're hearing about, the private programs from Radix and Donuts, in those cases the registry and registrar retains the determination of whether a complaint is specific and credible enough to be actionable. And on all of those elements, Jon and others will take discretion. They are not going to take an action -- as Steve indicated, an action of taking down an entire domain because one user has used that domain to post illegal content or, worse, selling counterfeit goods or stolen goods.

The specificity is essential, and I believe that you're more than likely to trust that Donuts is not about to strip down an entire domain because of the activity of one consumer nor would ICANN in its enforcement of the PIC specs do the same, because the PIC spec that PIC spec 11 describes has a parenthetical about consequences, consequences like suspension. And it says parenthetically, consistent with applicable law and any related procedures. The safeguards anticipate the need to balance the specificity and actionableness against unintended consequences to anyone else who might have used the domain for perfectly legitimate activity just because one person has taken an illegal action.

RAFIK DAMMAK: Okay, thanks Steve. So what we are going to try here is to get from Thomas and then from Mitch, and really we need to move to the next question because we still have like special questions that we have to cover. Thomas.

THOMAS RICKERT: Thanks very much, Rafik. My Thomas Rickert and I'm representing Eco, an internet industry association from Germany. And I've been asked to join this panel by the registrars because we have a 20-plus year history in helping the industry in self-regulation certain projects in the area of online safety and security. And I think that, listening to what all of you have said, I think many of us have different scenarios in mind, and that we might draw the wrong conclusions at times.

For -- I think this whole area is very complex and it forbids broad burst solutions because they just don't work. And it's not like an Internet service provider, a registry/registrar kicks out their customers easily. But they are in a predicament. In the legal regime that I'm living in, if you are notified as a service provider of illegal activity or services that are being offered and you don't do anything, you might be subject to criminal liability. At the same time, if you take down a service for your customer that is perfectly legitimate, then you might open yourself up to liability towards your customer.

So registries, registrars, ISPs, they want to do the right thing, but it's not always easy for them to do the right thing. And I think that there's a -- there are a couple of cases or a lot of cases where they are not making the right decisions. But all those that I don't -- that I know don't make these decisions lightly. So I've seen complaints like, I don't like what I see on the Internet. What do you do with that? Or more specifically, I don't like what I see on yahoo.com, right? So it doesn't work that way. You have to look at the cases one by one. And I've been responsible for the German equivalent to the IWF hotline or the NCMEC hotline, and I've been president of the Inhope Association which was the -- is the international umbrella organization of hotlines that works specifically in the area of reducing the availability of child sexual abuse images and try help find perpetrators and free victims, right? And the way that it's done there is you would vet those incoming complaints and then you would work with law enforcement, you would work with the ISP and try to take appropriate action. Sometimes you shouldn't take down a website or a domain name because there are ongoing investigations. Many of these websites that you see of material that I hope none of you will ever have to see is evidence of ongoing abuse. So just making that material invisible for certain parts of the users might not be the right thing. So taking this down might be the wrong reaction.

So we need to take a look at what is the complaint in question, what is the appropriate response. Is the registrar actually the right person to talk to, or should you rather talk to the ISP to take down a website and avoid further distribution of illegal material.

So all I'm saying is, self-regulation is great. Service providers have had their terms and conditions and acceptable use policies since the beginning of the Internet, and it's perfectly okay for them to lay out the rules for their own services. And if you as a customer are in breach of those rules, you have -- you are at the risk of the contract being terminated and your services being down. But it must be done with -- diligent, it must be done thoughtfully. And there are a couple of examples where this didn't happen. There are blocking lists that are being made available to ISPs for blocking and filtering, and some of these lists have been analyzed and some of the organizations aggregating those lists don't review the items on the list. So there's overblocking in certain areas. And also there needs to be accountability of those who are running the list. There has been an example in a northern European country a couple back where ISPs took filtering lists from law enforcement and then there was a customer with a website complaining to the ISP that his site could not be accessed. And then the ISP said, well, we have this MoU with law enforcement so we just take this list on an as is

basis and use it. And so we went to law enforcement, and law enforcement said, well, we're just making this filtering list as a way of recommendation so we're not taking responsible for it either.

So in all this, there needs to be diligence and due process. There needs to be a possibility to object to takedowns that have taken place. But all in all, I think, you know, if you take a nuanced approach, depending on the complaints that are coming in, it's perfectly okay for service providers to take down certain customer sites if they're in breach.

RAFIK DAMMAK: Okay, thanks, Thomas. I'm going to -- to Mitch. I think you have several comments, but please also be brief.

MITCH STOLTZ: I will, and thank you. I'm -- I'm for the most part heartened and encouraged by what I'm hearing here from the registrars and registries in terms of nuance and in terms of individual discretion. But here are my concerns, and I will give them in specifics to answer Michele's point. I'll give -- I'll give three. One was a proposal by the healthy domains initiative to create a basically UDRP for web content. The second, and this was -- we covered this on the FF blog, I encourage people to read this --

was enforcement of online pharmacies. Various groups calling for suspension of domain names of pharmacies primarily in Canada who under United States policy were actually permitted to ship pharmaceuticals for personal use to people in the United States. And -- in other words, a lawful or permitted transaction but according to a particular industry association's view of the world, those entities should not have the right to have a domain name. And the third one is the Donuts agreement with the MPAA. And I'm not -- I'm not picking on Donuts or on PIR for that matter because I think they are entitled to act within their discretion. But within days of the announcement of the Donuts/MPAA agreement I saw numerous comments, and I'm paraphrasing here, but what all of them said was, and let this be a model for everyone. MPAA itself said this comments to the United States trade representative and which this was mentioned in various think tanks and interest groups in Washington, DC were saying this. That's where the danger lies. Because while we can say well obviously some things are legal and some things are illegal and there -- this is a black and white thing, there's always enforcement discretion and there's always differences in interpretation. And if everyone is subject to the same policies, then they are effectively laws and that's effectively law making by other means. And the U.S. government itself -- again, I'm U.S.-focused, but I know there are other examples. This is outside of the domain name complex

but a similar one was the European Commission asking online content platforms, social networks and so on, to quote, voluntarily, unquote, enforce hate speech policies, which are, of course, not uniform from country to country and are fairly controversial in many countries. These sorts of things you cannot -- we cannot actually call these voluntary measures when governments are cheerleading them and pushing them with the -- you know, with the quiet threat of future legislation and regulation if they're not done. Those are not voluntary any more than they're -- you know, they're under threat or quiet threat.

Here's the broader point though, right? What is a domain name for? Is it simply a unique identifier for an Internet service? Or is it some kind of certification of good citizenship or legality? And if it's the latter, who decides? Who makes that certification? And under what country's laws and under what kind of policy? And if it is that and people disagree with that set, with that -- the content of that certification, then that -- doesn't that undermine the technical functioning of the Domain Name System? That is my fear.

RAFIK DAMMAK: Okay, thanks, Mitch. So -- okay, Liz, very brief.

LIZ FINBERG: Just really briefly, but I would be remiss if I did not state for the record that there has been no proposal within HDI for a UDRP for content. And with respect to various practices or proposals that touch pharma, I will tell you that there's not -- there's no pressure within HDI for all of its members to adopt the same practices. The point of HDI is that it is a non-ICANN industry-based group and these are purely voluntary practices and within the group there's -- there's -- there's very, very broad and general understanding that we don't agree and that we -- we will, you know -- each of us are free to adopt or not any of the proposals that are being discussed. Thanks.

RAFIK DAMMAK: Thanks, Liz. So let's move on to the next question, which is about can ICANN and other Domain Name System participants successfully participate in certain form of content regulation while refusing to participate in others. So this is maybe to expend more than just about copyright or misuse issues and so on. I would like here maybe to hear from those who didn't talk already, maybe starting with -- yes, Richard, that's you.

RICHARD LEANING: Yeah, Rich Leaning for the record. I'm here in personal capacity as an ex-law enforcement officer, the only one they could find walking through the building, on the way to the bar. It's an

interesting discussion, and from the law enforcement perspective, but it's -- as my colleague over there said, it's really, really complicated, and it's complicated for all law enforcement globally. And we tend to deal with all these issues on a national basis because that is where we're based and that's where the legislation is. It's interesting to hear what we do deal with registrars and registries and we build up good contacts with them. Someone like Donuts is saying they come across a case that involves something that is -- that is obviously against the regulation legislation, we'll go to the registrar and say look, we'll leave that to your decision.

The complication for us is that -- for law enforcement is do we talk just the domain name? Do we talk what Google finds? Or do we talk where we spend most of the time is in the dark and deep web which is not anywhere in this type of environment. That's completely different issue and then normally ccTLDs in a jurisdiction that none of us in law enforcement have got any control over whatsoever. So it's really challenging for us.

We deal with individual cases, and it's predominantly reactive. We'll try being more proactive but it's predominantly reactive and each one is dealt with on that particular case. The problem is everyone thinks cybercrime -- law enforcement deals with all cybercrime. It's not. The Internet has got the same crime on it as it has in the real world. And you -- there's not one unit that

deals with crime in the real world, so there's not one unit that deals with crime on the Internet. And each one has different practices, if its pharmacy, if it's child abuse, firearms, drugs, whatever that may be. There's a separate entity within the national jurisdiction that deals with it, and they deal with it different ways with the partnership and stakeholders that they have managed to work with to find what the best solution. And there's never a set solution for every scenario. It's different every single time, because that's the way the Internet is.

You know, on that question, yes we're aware. It's not something we as law enforcement really get involved in unless there's something that is brought to our attention that we, you know -- we do it because of that. You know, as we say, there's no -- there's no global law, there will never be a global law, and we deal it with -- in a national jurisdiction with our partners. I hope that -- I spoke anyway, so that's -- that's a start.

[Laughter]

RAFIK DAMMAK: Okay. So we'll listen from Shane and then Robin.

SHANE TEWS: Hey, I'm Shane Tews. First of all, let's do a reality check. It's 6:00 on a Sunday. We're in India in a historic, very beautiful place

and we're all in a cold, dark room talking about this topic because this is a community that takes getting the balance really as an important thing. That's why the RAA took so long. It's why the application guidebook for the new TLDs was such a strenuous exercise and as many of the people here at the table we're just part of the CWG or the CCWG trying to get the next layer of ICANN right.

So I think it's important that we all take a moment to realize this is a group of people that have really tried to make sure that we're not stepping on anyone's rights at any place. But the Internet is not a lawless place because it's digital. Companies should not have to host illegal or harmful activity. We saw that just recently in the United States with a Dyn attack. That was a voluntary effort to keep the Internet going when we saw an Anycast attack that was very challenging for some major companies. So taking action, even if its terms of service on an illegal or abusive activity under a voluntary agreement or a voluntary collaboration is a tool. And it helps keep the Internet safe and secure, and we're trying to manage the balance through all of this as we deal with harmful activities that are online. So as we manage abusive conduct, we're not removing content. We're using that ability to suspend a point of access while we manage the information that is being guided through the process.

So I -- I just want to commend everybody for taking the time to continue to try to work the balance on this. But the fact that individual companies have chosen different ways to work through this just reminds us that we have a choice in how this works. And this is not mandatory shadow regulation that everyone has to abide by.

RAFIK DAMMAK: Yes, Robin.

ROBIN GROSS: Thank you. Yeah, I mean, if we look at what the question is, it's really asking us how do we -- how do we participate in certain forms of regulation and not others. And I think what we're finding here is a conflation of all these different issues. There's really a slippery slope for the -- when you're talking about enforcing terms of service for registries and registrars. They don't really distinguish what we see up on the -- on the screen here. It will just say illegal content. And so I don't think there's anyone up here on this panel that's going to dispute the need to act quickly and effectively when we're talking about child images and things that talk about actual real world violence and harm and things like that.

So the problem is, that's the kind of argument that we're hearing. And then it gets applied to copyright. And then it gets applied to, you know, licensing and business and all these other things that have -- that are nowhere near the kind of harm, the kind of situation that we're talking about, if it were about child pornography and some of these other things. But what one of the risks we have when we start looking into these issues is really sort of expanding ICANN's mission. And a real mission creep. So now look at all of these different issues on the screen here. And ICANN and the contracted parties, they're all going to have to become experts and decide whether or not something is -- should be acceptable because it's a licensing issue in a particular jurisdiction or if it counts as blasphemy or if it's against public morals. I mean, this is an enormous amount of expertise and expansion of ICANN's mission far beyond just coordination of the Domain Name System. I mean, these are all legal issues, these are all policy, social, societal issues. These aren't coordination of the domain names systems.

So we've got this real conflation between what our terrible violent sort of harms that everybody agrees need to be acted on immediately and then using that argument to say oh, and we're going to take copyright down, too. So that's a big problem that we have.

JON NEVETT: Quick reply. Yeah, thank you, Robin, because that is a much more reasonable position than -- I just looked up from this form I guess was given out about the Manila principles. And principle Number 2 says, "Content must not be required to be restricted without an order by a judicial authority," period. It does not say, Well, we care about -- we don't care that much about copyright but child imagery abuse might fall under that or, you know, something else might fall under that. It's pretty strident.

Yeah, I could understand the view that you have. And I think it would be perfectly reasonable for a service provider to say, I'm not going to deal with copyright. They might decide to do that.

For us we decided for clear and pervasive cases when it is a clear-cut case, we would deal with illegal copyright material. And that was a choice that we made.

But to subscribe to these Manila principles would be really strong because I don't know of any service provider that would actually say, No, I'm going to make you go get a court order for child imaginary abuse or something like that. That's a more nuanced and reasonable position than others have made. So thank you.

RAFIK DAMMAK: Okay. Thanks, Jon.

Graeme?

GRAEME BUNTON: Hi, Graeme Bunton from Tucows. Looking at this question and thinking about the comments, I think Thomas captured a lot of this really nicely about the complexity that's involved in dealing with these sorts of cases. You know, especially on a day-to-day basis, if you go talk to any frontline compliance staff at a registrar, they're going to tell you that they hate making choices. They much prefer that those choices are made elsewhere.

It's mostly because we are not good at figuring out what's a violation of law or not. It's much beyond the capacity of a registrar to do that.

And I will say that everyone thinks that their abuse complaint is super clear-cut, and that's not the case when you are digging into most of them. There is gray areas in almost every single abuse complaint that we see that requires sorting out. Tucows approaches this in a number of ways. One is we try and get people -- the complainants, the registrant and the abuse complainant, to actually communicate with each other and try and resolve that issue on their own.

For us, we see ourselves as keepers of process. You know, we try and not have to make that choice but ensure that process is

followed all the way through and that we feel that process is clean. We can look at ourselves in the mirror the next day.

For us where the rubber meets the road on a lot of abuse issues, we really do try and ensure that due process is followed. Kind of like Robin, I try not to conflate the exigent circumstances issues, which is like where there's imminent material harm to a human with some of the rest of the abuse complaints that we see.

You know, and we do -- we get lots of what look like very legitimate complaints that are not once we start digging into them, fake law enforcement requests. And so the burden is that you really have to dig down into the weeds on every single thing. And it's time consuming.

I get -- and I think it makes business sense to do what, say, Jon is doing. It's faster. It's easier and doesn't require as much work. I don't think it's wrong to do that. I think there's other ways to approach it, which we try and do with a fair hand. We don't always get it right, but I think we feel generally pretty good about how we approach these things.

RAFIK DAMMAK: Thanks, Graeme.

I think Steve DelBianco and then we go to Mitch, yeah.

STEVE DelBIANCO: Yeah. I like the way that this question is phrased because it gives me an opportunity to say that I want to be Mitch's ally because my day job at NetChoice is to make the Internet safe for free enterprise and free expression for my corporate members. And that means Mitch and I both lobbying like crazy to stop a legislature or national government from passing a law that's completely unworkable with cross-border Internet commerce and content. So, for instance, laws about government criticism, laws outlawing hate speech, the infamous right to be forgotten and restrictions on data flows, these are the kind of laws that we should work together to oppose.

We won't always succeed, Mitch. And when we fail, we turn to the second part of your question.

We need to be sure that companies that exercise their own programs have the discretion to act upon complaints that come in based on the procedures that they have, so discretion at Donuts is a good thing.

And what about ICANN when it comes to enforcement of the PIC spec? The good news is that parenthetical that it's about considering applicable law and any related procedures. So those related procedures are the opening for all of these contract parties to say that our related procedures with respect to a complaint about this hate speech is to demand the level of

specificity and the verifiable nature that that speech is there and that it, in fact, violates the law. So that is how you're able to gate this and avoid some slippery slope to suggest that a simple email from a government official is tantamount to forcing you to take down an entire website.

All of us working in this industry have to require that with laws that are really unworkable or, in this case, many of them unwise, sometimes they'll pass. But it's not incumbent on you to act without procedures and balanced against other aspects of applicable law. So I look forward to lobbying with you, Mitch, across the world.

MITCH STOLTZ: As am I, Steve. Thanks.

Child abuse imagery is a poor example. And I can tell you why and give an example of the problem here again. This is outside of the Domain Name System but very closely related.

A voluntary system in the United Kingdom at the ISP level for blocking child abuse imagery was set up. And then the entertainment industry said, Oh, we have this great system in place. And so now we can use it for copyright infringement. That's where it starts.

And I will give another example again outside of the Domain Name System but illustrative. And that's a system that is in many ways similar, which is the Motion Picture Association of America's ratings board. This is the preeminent film rating system in the United States, which like ICANN is a non-governmental organization that does not wield the power of law but nonetheless has a great deal of influence over what people can ultimately see and hear as far as films. They were recently sued in a class action lawsuit in which a group of consumers demanded that they use the influence of their ratings board to essentially prevent children from seeing any imagery of tobacco use.

And the MPAA responded in court, and I think correctly, that they can't be compelled to do that, that that's not what their system was set up to do and that they should be able to use their own judgment.

But when you have a mechanism that can interrupt speech, that can prevent people from -- can block the channels of information, people will come in and try to use it for all of these purposes, good and bad, right and wrong, and with differing priorities. That's where the danger lies and that's where ICANN, in particular, I think needs to stay far away from this.

I am an outsider to ICANN. I will admit this. I'm not a regular participant. But to me regulation of content is regulation of content, and it doesn't matter if we call it a PIC or we call it something else. But if it is -- if it is unavoidable, if it is something that in a practical sense applies to everyone, then it is the equivalent of law.

RAFIK DAMMAK: So I have a suggestion. So we have 15 minutes left in this session. We will try to get just one to intervene and then we try to open the floor for the audience to see if they may have question or they want to intervene. So we will go with Allen and then Steve Metalitz.

ALLEN GROGAN: I will try to keep it brief. So since one of the questions here was: Can ICANN successfully treat content regulation in certain areas differently than others, I wanted to make two observations going back to where I started, mission and bylaws and contract provisions.

So on the new mission and bylaws, part of what is now expressly within the scope of ICANN's remit is to coordinate the development and implementation of policies for which uniform

or coordinated resolution is reasonably necessary to facilitate security and/or stability of the DNS, among other things.

So I think when it comes to policy development, you could look at the mission statement and conclude that certain kinds of abuse to the extent that they implicate stability and security of the DNS may properly be the subject of policy development that could lead to ICANN having greater rights of enforcement in those areas.

So, for example, if you were talking about malware or botnets that could potentially impact the stability and security of the DNS as a whole or that could take out the root servers, that may be squarely within the scope of ICANN's mission and remit. And, again, that's properly subject to the development of policies through the multistakeholder bottom-up process, not through ICANN staff imposing that.

But if the community decides to develop policies that relate to forms of abuse that directly impact security and stability of the DNS, I think that's arguably squarely within the scope of ICANN's mission and remit.

And then just briefly on the contract side -- and this is all complicated, which is the reason I didn't want to go through all the contract provisions. But one of the challenges, I think -- and, again, I think it's partly a matter of policy and partly a matter of

where are these decisions properly made. Are they properly made by ICANN staff, or are they properly made through the multistakeholder process? Some of the provisions in the agreement, like Section 3(a) of spec 11 of the New gTLD Registry Agreement require provisions to be included in contracts with registrants that prohibit a laundry list of activities: Operating botnets, phishing, piracy, trademark or copyright infringement, fraudulent and/or deceptive practices, counterfeiting, or otherwise engaging in any activity contradictory to applicable law.

I think it's a legitimate question as to whether when you have a laundry list of activities like that, is there any basis for ICANN to say, You should treat some of those activities differently than you treat others, or is that a matter for the community to determine rather than for ICANN to determine?

And I'm not answering that question. I'm posing the question.

RAFIK DAMMAK: Okay. Thanks, Allen.

So we will go to Steve Metalitz. This time you will have to be brief. Sorry for that so we can go to the audience.

STEVE METALITZ: Yes, thank you. Steve Metalitz.

First, on this question, several people have said we have to be careful and diligent and recognize the nuances. And I agree with that. Let's look at this question in that light with the issue of conflation. First of all, as I said in the very first intervention, if ICANN can do it or if Domain Name System participants can do are two very things. The ICANN question is governed by the contracts and the consensus policies in terms of what they can enforce. Domain Name System participants, registrars, registries, and others, I think we've -- a lot of people have said there should be a lot more encouragement or flexibility for them to set their own policies and to enforce them. So that's one conflation we have to worry about.

Content regulation, let's be clear, governments regulate content. This is not about content regulation. This is about enforcing terms of service that have -- that prohibit the use of your services to carry out illegal activities that may involve in some cases certain kinds of content. But let's be careful with the labels that we apply to this.

And, finally, on the slippery slope question, which I think is certainly a legitimate concern, so I think we need to be thinking about ways -- maybe there are some handholds that can be used to help reduce the slipperiness of the slope.

One measuring stick that can be used -- and this is kind of a legal analysis -- is how widespread and universally accepted are the global legal norms in a particular area? And I think you can distinguish between things like blasphemy where obviously there is no international legal norm about what blasphemy laws are permissible and not permissible and something like copyright where 160 -- I think 172 countries belong to the Berne Convention, which is the premier international copyright convention, 164 countries belong to the World Trade Organization TRIPS agreement which sets not only standards for copyright protection but enforcement standards. It's not that these countries all have the same laws because they don't, but there is a very high level of legal harmonization which I think puts you in a different place on the slippery slope than in blasphemy. And the malware situation actually from a legal standpoint falls somewhere in between. There is much less adherence to any international legal norms with regard to malware than there is, for example, with regard to copyright.

But there are also are some pretty well-established voluntarily arrangements, malware organizations, some of the lists that have been talked about that are pretty widely accepted and that may provide a good way for carrying this out in a way that's nuanced and focused. Thank you.

RAFIK DAMMAK: Okay. Thanks, Steve. We'll go now to the question from the audience and we'll ask, again, please be brief, as much as possible. Please state your name and your affiliation.

MILTON MUELLER: Right. Milton Mueller, noncommercial users constituency and Georgia Institute of Technology.

Steve, you accused EFF of blurring the line between ICANN-imposed contractual provisions and private terms of service, and I actually think that that's true. Mitch did that, to his detriment. But I think that the registry and registrar participants and the IPC participants have done the exact same thing in reverse. You've given us the impression that it's all private and variable and everybody has plenty of freedom to choose between different terms of service and there's no law or governance being imposed on anyone, and I think that's equally false.

In fact, you both seem to have missed the degree to which we are using ICANN to leverage various forms of content regulation.

And finally, Mr. Grogan started talking about Section 3(a) of Spec 11 in some detail, and what is that, gentlemen and ladies, if that is not a fairly detailed attempt to leverage the domain name

system to regulate various forms of activity that are not directly related to the security and stability of the domain name system?

Why, indeed, were the IPC and the registrars and registries, Jon, still having debates about ICANN's role in enforcing spec 11? What about this laundry list of activities? How much of that is directly related?

We need to have a much more focused discussion of ICANN's role and the dangers of it spilling over into content regulation. Thank you.

PATRICK PENNINCKX: Yes. Thank you. Thank you for this extremely interesting discussion. I found it extremely interesting. My name is Patrick Penninckx. I come from the Information Society Department of the Council of Europe, and, well, I did think that the discussion was maybe a little bit too much U.S.-centered and maybe you will -- may be a bit too much U.S.-centered, and thank you for the German participant to also bring in the views of the German authorities in that.

Now, in a number of cases, I don't agree that name registration and content regulation do not go hand in hand. You have yourselves, as a panel, given examples of where the name of a Web site is sufficiently clear to what the content that you can --

that you can expect behind the name of that Web site. So I think it's also clear -- interesting and important to know what we are talking about.

Now, when it comes to avoiding content regulation, it's all fine, but what do we obtain as an end result? That is, the diversity of interpretations and the unclarity and legal unpredictability of what the roles of ISPs is going to be. And this is not only in the U.S. context but also in the context -- in the European context. For example, where I come from, it's interpretations of the European Court of Human Rights or the European Court of Justice which will look more precisely and maybe give responsibility, as the German colleague said, criminal liability, of ISPs in this context.

And I think this legal unpredictability which, of course, flows from everyone applies its own principles, can also have a chilling effect. It's not only a question of taking down Web sites or other, it's also the chilling effect of the total legal unpredictability and climate in which we live.

And one answer to the no international instrument regarding cybercrime-related activities, there is of course a cybercrime convention, the Budapest Convention, which already has 50 states which have ratified the convention but 125 countries that

are following the implementation of that convention. Thank you.

LEON SANCHEZ: Hello. My name is Leon Sanchez. I'm from the ALAC and also a member of the IPC and it strikes me as a little bit contradictory that EFF is here asking us to give up our freedom to freely contract between parties. That's at least my impression.

And it also strikes me as surprising that EFF is trying to do what it fights against, which is export U.S. law. Because when you tax all jurisdictions under the same law as the one that -- that applies to the U.S., it seems to me that you are trying to export U.S. law, which is what you actually fight against, and that's -- that's something that I would like you to explain to me, if you're so kind.

And also, I would like to know how do you see your -- how do you understand, how does enforcing one's rights impose any burden on ICANN on regulating content?

I -- it seems to me that you see copyright enforcement as something wrong. It's as if a rights holder shouldn't be able to enforce its rights, and I think that copyright is as important as freedom of speech and as other rights. I mean, you shouldn't be putting different levels on fundamental rights, as far as my

understanding goes. But those are the questions that I want to pose for you specifically. Thanks.

KATHRYN KLEIMAN: Anybody want to respond? Okay.

MITCH STOLTZ: I'll be happy to respond but I'll wait because I want everyone to have a chance to ask their questions.

KATHRYN KLEIMAN: Kathy Kleiman, noncommercial stakeholders group.

So Mr. Grogan wrote in his blog that -- in 2015 that ICANN is not a global regulator of Internet content, and the board affirmed that this morning in a meeting with the NCSG.

And so you're doing it privately. Congratulations. You're going behind closed doors without the noncommercial community there, without the representatives of human rights and public interest and you're negotiating private policies that don't have due process, that aren't fair.

So I heard Mason Cole, in front of -- in Helsinki. He was there as the GAC/GNSO liaison and he was presenting the Healthy Domains Initiative as if it was a multistakeholder policy. Guys, the DNA is a private organization and we weren't there. The

noncommercial community wasn't there and the policies aren't fair. God knows the MPAA and Donuts agreement isn't fair.

Steve, you're right. Copyright law is international, it's global, it's in lots of countries, but how do you -- but do you know copyright infringement when you see it? There's still a process for declaring when something's illegal. And I don't know, I'm not judge, jury, and executioner and I wasn't when I was a gTLD as .ORG. Sure we took down phishing, sure took down botnets. These were threats to the security and stability of the DNS. You guys are going way beyond that and, yes, there's going to be a pushback particularly against the registries who are newly engaged in this content regulation. You're doing it privately, you're doing it without due process, you're doing it without balance, and in a lot of ways you're presenting it as if it were part of the multistakeholder -- as if it was a multistakeholder product and it's not. We beat SOPA and this is SOPA behind closed doors. Thank you.

RAFIK DAMMAK: Thanks.

MITCH STOLTZ: Yeah, if I could jump in -- yes?

RAFIK DAMMAK: Just to say that we closed the queue, and yeah. We are closing the queue for the audience so finish the question.

MITCH STOLTZ: Thanks, Kathy, and thank you, Mr. -- I'm sorry, was it Sanchez? I will try to answer your points.

I apologize that most of my examples come from the U.S. That is -- that is my area of expertise and I'm glad that others on the panel have filled in from the rest of the world. That is -- that's helpful to the -- to the discussion. But I'm not asking for an export of U.S. law. I'm talking about principles that -- that I think are fundamental to the Internet or fundamental to the -- many of the members of this ICANN community who -- who, you know, in a very real sense built the Internet. And that is that speech is the prerequisite for -- that guarantees all other rights and a political process and forum in which we can begin to debate and form those other rights. And I mean, engineers and technical folks will understand this particularly because restrictions on speech are restrictions on the flow of information, the exact thing that the Internet was designed to avoid. There's a strong link here between the regulation of content and blocking the channels of communication.

So, no, I don't say copyright is something wrong and I -- and I acknowledge that copyright is -- obviously exists in most countries. It is certainly not uniform.

I'd add as a counterexample hate speech laws are in a lot of countries -- certainly most of Europe -- and yet they are controversial, they are difficult to apply, and they depend strongly on who is applying.

So I take this back to -- and this was in the -- in the questions: What is a domain name for? Is it a -- is it a certificate of good citizenship, is it a license to speak on the Internet, or is it simply a unique identifier?

I think for this community, you know, a guiding principle -- and I'm not insensitive to nuance here or particularly to exigent circumstances. I agree that any participant in the system should be able to respond to exigent circumstances. But -- but our guiding principle needs to be -- needs to be free expression.

RAFIK DAMMAK: Thanks, Mitch. So we will get the -- the two last questions and we will have really just an extra five minutes just to last comments but let's get -- they were waiting, yeah.

GERTRUDE LEVINE: Thank you. My name is Gertrude Levine. I work for the National Association of Boards of Pharmacy and we are the registry operator for the .PHARMACY gTLD and I wanted to point out to the group that NABP has reviewed over 10,000 Web sites selling prescription drugs to U.S. patients and that 96% of them have been found to be operating illegally and 80% of them are selling prescription drugs without a valid prescription. That means without medical oversight, without the guidance of a pharmacy, with a -- without a pharmacist.

And without even getting into copyright law or whether -- or the fact that it's not legal in the United States to import drugs from Canada, it's clearly against U.S. law to sell prescription drugs without a valid prescription by someone other than a pharmacist.

The RAA specifically says "all applicable laws," and I don't believe that it is up to the ICANN community to determine what's an applicable law or which applicable laws that they will follow and which they won't. They're obligated to follow the laws, and that was the decision of the ICANN community to adopt the RAA because it's the right thing to do.

MITCH STOLTZ: So all the laws of all the countries?

GERTRUDE LEVINE: In the countries where they are based and where they operate, yes.

RAFIK DAMMAK: Thanks. Thanks. Mitch, let's -- sorry, Mitch. Let's get the last question because I think there are several speakers who want just to make last interventions.

SAVIO DSOUZA: Hello. My name is Savio Dsouza and I'm from India. This is the first time I'm at ICANN. I am the secretary-general with the Indian music industry which represents about 65% of music in India, and each year when the 301 report is written, India ranks very high on piracy. India ranks very high on piracy currently because of the digital content that is available and it's available freely. We are not able to do anything to stop this content that is available on the ground.

When I came here for this conference for the first time, I had no idea why I'm coming here or what I'm going to get out of it, but I say that I'm pleased to know that ICANN is keen on inviting newer people to join the ICANN, we hear about things that are happening at the ICANN, and take it back. I thought that was very positive.

I was very happy to hear both the union ministers, the minister for state and the minister of center who spoke yesterday and volunteered to support any issues that ICANN had, including dealing with infringement of copyright.

And those were the positives that I had.

But as I've been here for two days, I've heard so many statements coming along this room that say "I don't think ICANN should enforce the law," "I don't think there should be self-regulation," "I don't think governments should regulate." There are people who even said that.

And when I hear this, I go back very unsure what I should tell my constituents. The ICANN is a nice place, they call us in, they're welcoming us in, but there are no solutions on the ground.

And if you want to welcome India, China, the other countries move it from being U.S. centric and Europe centric, then we need to find some solutions that can work for us on the ground.

RAFIK DAMMAK: Thanks. I know that there are several people who want to respond.

We start with Jon.

JON NEVETT: Thank you. Jon Nevett. It's unfortunate Kathy just walked out because she is just plain wrong about the healthy domains initiative. This is an industry association, industry-led initiative. It has absolutely nothing to do with the multistakeholder model. In fact, we -- like I said from the start, we don't believe in ICANN regulation of content. We don't think these should be mandatory. We think these are voluntary initiatives that registries and registrars should take up, if they should choose to do so. We think they are good ideas. For example, establishing a relationship with NCMEC, you know, the child imagery abuse entity. That's a good thing to do. We recommend all registries and registrars have that kind of relationship, or the IWF and other similar entities. This is not multistakeholderism.

And second point is she said this was done behind closed doors or trusted notifier program not with NCMEC but trusted notifier with MPAA. The opposite is we announced it. We went public. We have a blog post with what kinds of referrals we have been getting and what we have done with those referrals. We have been totally transparent about it. And so to say that was done behind closed doors without transparency is, again, just plain wrong.

So, you know, we've provided due process in those cases, and we will continue to do so, and we will continue to be transparent. Thank you.

RAFIK DAMMAK: Thanks, Jon.

Michele.

MICHELE NEYLON: Thanks, Rafik. I'm going to have to run. So if I run out it's not because I'm scared of any rebuttal. It's just I have to be somewhere else.

Look, I think this kind of conversation and dialogue is great to have because it is important for everybody to understand the boundaries of what falls within ICANN's remit. Personally, I've been involved in industry and Internet kind of governance-type debates for years. One of the things I have always felt is key is that we as an industry self-regulate that we have self-determination and that we are able to choose how we want to run our businesses in order to have a free and open Internet, which is something I think most of us are in favor of. However, the reality is in the real world people do bad things on the Internet. And personally I don't -- I would not be able to sleep at night if I felt that either through my company's inactions we led something that were to happen that were to lead to harm. And I'm talking real harm, not the harm to some brand. I'm talking about people actually dying.

So, for example, when it comes to things like, say, fake pharma, my company has voluntarily entered into an agreement with LegitScript. And I will quite happily stand over it.

I do not see the ability for somebody to sell fake pharma online as having anything to do with speech. It's dangerous, and I do not want to have anything to do with that.

As for the HDI initiative, my company is not a member of the DNA. And I have not been quite vocal about not being a member of the DNA. However, I have been involved with the HDI and many other anti-abuse initiatives for the last I don't know how many years. And I will continue to do so for the reasons already stated.

If we don't clean up our own act, then we will end up in a situation where governments start to regulate us. And that is going to lead to much, much, much more pain and to a much nastier situation.

And for anyone who wants to continue the conversation with me or anybody else, I'm not hard to find. Thanks but I have to run.

RAFIK DAMMAK: Thanks, Michele.

Steve?

STEVE DelBIANCO: Yeah, just ten seconds here. Mitch cited as an example that U.K. Internet service providers were blocking child porn and that since that might be cited as an example for trademark and copyright that we, therefore, should not block child porn at all. I can't conceive that that's really what EFF is thinking, and I'm looking forward offline -- we're out of time today. But I look forward to understanding how we do good things and avoid having it become slippery slope to things that EFF is wanting to avoid.

MITCH STOLTZ: Again, I'm heartened by what I've heard here today, particularly from the contracted parties who I think have shown a commitment to avoid the slippery slope which is real and I have given several examples of it.

I'm still a little concerned about shadow regulation, by which I mean unaccountable regulation through private agreements which, again, are equivalent to regulation if they are imposed on the populous indiscriminately and without the choice that competition brings.

So if the healthy domains initiative has nothing to do with the multistakeholder model, then it should not be holding private meetings at this conference on ICANN's dime. And its products, its output should never be considered part of the bottom-up multistakeholder process. That is a dangerous path to follow.

Again, I think a guide for this -- Steve mentioned the Manila principles, and I encourage everyone to look at this. It's manilaprinciples,org. It was signed on by several dozen NGOs and public interest organizations from dozens of countries. And it does not say anything about self-regulation. The principle that Steve mentioned earlier is content must not be required to be restricted without an order by a judicial authority. It's not required to be. That's the difference between a company choosing how it does business and unaccountable regulation, whether that requirement comes from a government or from ICANN or from a private collusion. It's really I think an informative set of guiding principles.

I'm very happy to be here. Thank ICANN for this opportunity and thank everyone on this panel, for this interesting and enlightening discussion.

RAFIK DAMMAK: Thanks, Mitch.

I can take the blame for the time management. It is not one of my best skills. But I want to thank all the panelists because we spent time to work on this session. I hope that we will continue the discussion. It is just the starting. It is better that we -- we have such debate even if it is agree on different points, but we can work out on this issue. Thanks again.

[END OF TRANSCRIPTION]