Transcript for Plenary 2 – Room 305 – International Law Enforcement

Track 3(b) International Law Enforcement

Site: Suntec Singapore International Convention and Exhibition Centre, Room 303

Date: 17 June 2011

Start: 11.00a.m

End: 12.30p.m

Chair: Pablo Hinojosa

Panelists: Pablo Hinojosa, Sharil Tarmizi, Hong Xue and Jordan Carter

CHAIR: Pablo Hinojosa

I'm honored to be the chair of this session on International Law enforcement. We're here in the room actually, but this session is being broadcasted, so probably we can generate good discussion material to put in the notes for them to be part of the summary for the proceedings of the meeting. We are at the Regional Internet Governance Forum, governance refers to norms, rules and procedures, and internet governances has revolved around the decision making model and the multi-stakeholder model to give a consensus on the future of the internet. Enforcement is a different process and follows different logic. It is mostly a flying existing goals and mostly this can be done in a particular jurisdiction or on a national basis. As the internet has grown, it has on one side it has defined its future to a great and working governance model, on the other hand it has brought with it few evidence that has challenged the laws and governments. Cyber threats, privacy challenges and battles protect intellectual property rights affect all internet stakeholders. How governments can enforce the law at an international level when threats happen online, how governments coordinate internationally when there are cross border legal issues at stake, how can law enforcement agencies utilize the experience of multi-stakeholders in the internet ecosystem to work together to address cross border internet related with just national law. So this is the subject matter of this panel. We have a group of great speakers, so I am sure we will give Rachel, not only for the few of you that are here, but also for those

following us remotely, and for the posterity as well. So please if you would like to comment and contribute to the debate you are welcome to do so.

I will introduce now a very dear friend who I'm happy to see after a few years. Sharil Tarmizi is the CEO of the Malaysian Communications and Multimedia Commission. I had the opportunity to visit his office in Kuala Lumpur just a day or so after they were inaugurated, beautiful building. I met him more than a decade ago in the governmental advisory committee of ICAN, few years later he became the chairman of ICAN and we live together the hall of which is process from Geneva to Tunis. I can share many good anecdotes, memories of Sharil, but I will just leave you with one. I think he is best to tell you the story of the 3 blind men in front of the elephant and sharing the impression of the elephant from different angles. I think the elephant obviously is a great image to apply to the concept of internet governance. Ask him to tell you the story, it's a great image, with you, Sharil.

Sharil Tarmizi
Thank you Pablo. 10 years of friendship all you remember is 3 blind mice and an elephant. Those guys on my right you can hear me ok, is there a feedback that someone taking? Okay alright, you're probably wondering, a very good morning, a very enthused crowd we have in this room. I just want to get a sense, how many of you are law enforcement officials, anyone? How many of you have worked with law enforcement agents? (No one raises their hands) Then what are you doing in this camp? Experiencing. The reason why I asked is because I'm going to try and also share some very real examples. I grew up with the internet community, with a lot of friends around the room. Izumi at the back there, Pablo, Gordon, Professor. Anyway, there are a lot of things I learnt and there are a lot of things that they didn't know about what I did also.

I'm actually a law enforcement official. (Silence) Okay, no one knows, this is going to be tough. Usually there is a certain perception and perspective and I'll come to that in a bit, but when we're talking about law enforcement, different people will have a different perspective of what that means, particularly in the cyber world. And perhaps this is also

a useful time for me to also declare, because I have also other hats that I wear. I purposely left the affiliations on the slides blank. So I work for the government regulator in Malaysia, we do the kind of work that the FBI and the FCC do, combined. I also have an affiliation with an international multi-lateral organization which I sit on the advisory board and the management board, which I will introduce later. And I am also on the panel of another multi-stakeholder group.

Now I think we all in this room know about this, today even in the most remote of places in this world, you have to agree that ICT have become an integral part of society, and if 10 years ago everyone was looking at roads, electricity, water and basic infrastructure, now almost every government in the world is announcing a national broadband plan, every government is announcing a national broadband initiation, as well as measures to actually improve ICT infrastructure. But at the same time this is exposing us to things like cyberwars, cyberattacks and I think we've seen some in the past. And this is where the issue of vulnerability of national infrastructure increases. We now have seen, like in the last couple of weeks, last couple of months, cyberattacks taking place in many many places and launched from anyway. Now that statement below, at the bottom of the slide, you'll definitely agree with me that today there's definitely no geographical borders anymore, no boundaries and potentially there's tremendous destructive power. However, are we talking about the same thing when we talk about this issue, when we're in this track looking at issues of law enforcement?

You know, some people call the thing cyber security, what we understand by cyber security? I tried Googling for a definition, I didn't find much but I found links to other places and other things, but I'm going to share with you how I look at the issue, cyber security as opposed to cybercrime. I like to call it cyber threats, and I'll go on to share with you why, because I think it's got to do with how things have developed in the past, how recent history has shown us the kind of things that have come up from one end or another. But typically, when someone mentions cyber security, I think there is almost an instant gravitation towards things viruses and Trojans and stuff that computer engineers look at, geeks look at. But when you start talking about cybercrime then you

start looking at issues that typically the law enforcement officials start looking at, the guys who carry the guns, you know. I mean, this is my simple way of trying to put this together, but collectively their both cyber threats. Now, more on the same thing, if you're looking at threats there are many many type of threats, threats against a person, threats against an organization, sometimes it's a prank, sometimes it's malicious, sometimes it's targeted and personal, sometimes is accidental, sometimes data is lost or stolen, sometimes it's just an annoyance factor, sometimes worse, and a lot worse. We have not yet fortunately in Malaysia seen anything from cybercrime or cyber threats that have resulted in death, but I think you can read in other parts of the world, some of these things do happen.

Now that raises the question, at which point is it the job of the computer geek, at which point is it the job of the cop? If you're looking at the left side of the example I gave you, you know the virus, the Trojans, the botnets, the DDos, Spam, that is potentially, if you use, if for example if you inject a virus in someone's network and you harm that person's network, that is a crime, in a think, in fact a number of jurisdictions now. When that happens, and sometimes you were experimenting, you may be experiment, it's never intended, but it's a crime, you know instead of being in the geek environment someone in the gun carrying environment gets all excited because you just knocked down someone's network. Spamming, DDoS attacks, these are some examples where many of us who come up in the internet community or internet environment, you don't see these thinks that necessarily something that law enforcement officials will gravitate to? But they are and have become tools that are being used increasingly by, I'm struggling to find a term, unethical people I think, who are up to no good, online? And they are using these things to actually do something 'fouless'. Usually you have a going Trojan in and what they're actually trying to do is scrape of the data at the back end of your servers, because the real crime that's going to happened is credit card fraud, for example. Then there's the second category of the crime, which is a little bit more disturbing. Again through the same methods, in fact through things like IM, through twitter, through facebook, stuff that we use very innocently, and that's grooming and stalking, second example. I'm assuming you understand the terms grooming and

stalking? Are you guys familiar with it? (Silence) Okay, you guys know phishing and farming right, I don't have to tell you guys what phishing and farming is? I'm sure you do. (Silence) Okay you don't, okay. Alright. Phishing and farming is basically in the identity theft category, where people are assuming the persona or the legal, digital identity of a person, and very often that happens, you know we've seen cases, in some that we've investigated, people are more careful with the money in their wallet than they are with their password of their bank account, can I put it that way? So, many of them will write their password of their bank account on a slip of a paper and stick it to the back of their ATM card, sometimes. Or they stick it to their wallet and they go "pin number," and they go "access, password," something that simple. Sometimes it's something more nefarious, you get all this spam coming in, "your bank account has identified that your account has been compromised, please click here," and it redirects you to a site that has been compromised or phished. And then "please key in your details," and "please key in your user name, your password," and then next thing you know boom, $4000 is out from your account.

We've been investigating those cases with the police quite a bit, and a lot of it has to do with, again, is there anything the authorities can do about it, personally I don't think so. It's educating people, and I'm come back to that more. But grooming and stalking is becoming increasingly disturbing, and that's where kids nowadays, you know Facebook has a policy, nobody below the age of 13 can go on Facebook, but I know kids as young as 7 who have a Facebook page. And they are sometimes stalked, or preyed upon, by people who aren't necessarily pedophiles, some of them are pedophiles, but some are people who are out to take advantage on the kids or out to find information about the family. So this person goes online, over an IM chat, or through one of those 'poke' things on Facebook, says "Hello hi poke, I from the other school, I'm this age", but actually it's somebody else. Children being children, they're quite free with information and they'll quite happily share stuff, what mom is doing what dad is doing, next thing you know, someone in the family is kidnap or something worse happens.

Again we're seeing that because I think there are many instances where children are being very naïve and very innocent? They do not necessarily always ask their parents what they are doing or tell what their parents are doing online, And I don't like it though, I have to actually look at what they're doing. but then they can fall prey to these people. Now if nothing happens there is no crime, therefore law enforcement and people like me don't get involved. But if suddenly the kid goes missing because the kid has been kidnapped, or worse. Then the criminal element comes in and people like us start to have to trace through logs, data records and stuff, that's we have to work with ISPs for example to start tracing where all this started. A lot of crunching of data as well. Then there is another category of stealing data. You get a lot of stories about people hacking into systems, banking systems, online portals which have transactions where credit card details, personal details are stolen, where money is stolen. Now this category of context, stealing context, it's a little bit more contentious. Stealing content, breaching copyright, intellectual copyright including illegally downloading music, technically is an offence, in many jurisdictions. I think Jordan will be speaking more about it, especially the New Zealand case, I think Jordan will be speaking on the cross border side of it, so I'm not going to touch on it. So if we have to come back we'll come back to that issue, and then of course there's the far end of this threat landscape, where we're talking about stuff you see in the movies, where somebody hacks into a system ,compromises the system, takes over critical networks, planes go down, dams go burst. (Chair signals)

Ok he's signaling, yes Pablo, three more slides, thank you. And critical systems are compromised. Now a lot of the challenges we have faced, and I know I've been in this for about 10 years in and out. There is a lack of adequate and incomparable national and regional legal framework. There are just no laws to cover this, the existing laws will cover the offence at the end, but it may not necessarily cover the offence at the commissioning, at the start. Sometimes there is a lack of secure software, ICT applications. Very very few governments and countries have got the organizational structure to deal with cyber incidents. Usually it's after the act kind of thing? And information security personnel are also somewhat slacking in a lot of governmental institutions because the expertise is not always with the governing eyes. And also

international corporations can be quite tricky, I can tell you that in some jurisdictions before they'll help you give you an IP address, they'll say "where's your mutual legal assistance application which has to be done via the foreign office?" Alright that takes 3 days, if you're lucky. If that doesn't happen then the guy has wiped out his traces already and that's the end of that. So with all these challenges it is sometimes quite a wonder how, you know, I was in New York with a couple of police guys and they managed to track down a credit card fraud ring from a country in Eastern Europe where we were involved and it looked as if it was coming through Malaysia. And turns out they were defrauding people whose credit card accounts were in the USA. Mastermind in a European country, through a third country, in the US.

Now, what can we do, and this is only the tip of the iceberg, I have 10 minutes, and I won't be able to cover that much but everything's online. Law enforcement guys like me who don't necessarily find the internet a natural thing, I have to learn, and one suggestion is finding common areas to work together. And this is where perhaps I'll share with you the three blind men and the elephant. Anybody heard that story? Some of you know. Very quickly, there's an old tale, I think it's an Indian tale, 3 blind men looking at the elephant and saying, one is looking at the elephant from the front, and of course he can't see, and he's feeling with his hands, and he's saying the elephant is pretty much like a boa constrictor, a snake, a big python. Blind men number 2 says, and he's coming from the side of the elephant and says "no no no you're wrong, the elephant is actually like a wall," because he's touching the elephant this way. Blind man number 3 comes along and he touches the elephant from the tail and feels this twig like thing and he says "no you are both wrong, the elephant is like a twig." Each one of them is right, but for their perspective, but they are all 3 wrong, from the perspective of what the elephant looks like. Why that's relevant to keep in mind I think is that very often when you get into a situation where you have to find common areas to work together, there's a tendency for everyone to want to insert their own view of the situation, their own view of the environment. And that is not necessarily helping in dealing with a situation you're dealing with something you don't know.

So more often than not, I find personally that bringing together and coming together in an equal footing, in a multi-stakeholder environment is very helpful. For example, a lot of the tech guys who helped out in some of the stuff we had to do, if they didn't share with us what we could glean from some of the records we would never know to find the leads to other things. But if we didn't share how some of our methodologies in hunting down criminals, they wouldn't know what to look for. This I think Izumi in an earlier session had said, "only happens when there is mutual respect and trust with one another."

I'm going to give you 2 examples before I go off. One is a formal structure that was set up by the UN actually, this organization called Impact. What it tries to do is it tries to bring together academia, governments and industry experts to deal with cyber threats. But these are the guys that deal with the left side of cyber threats, the phishing, the botnets, the Trojans and the stuff that you see all these demon servers who operate out of some third/forth country. They try and deal with that when they actually got a global response centre and they exchange information. There are other groups that do this also, I think there is also First in US among the cert. But this is the first formal one under the UN structure. So guys from the developing countries may be useful to take note of this and find who your contact point is back home. There are 133 countries who have joined IT Impact coalition, under oath, so it'll be useful to know who your rep back home is. Basically what it is is to deal some of the challenges I mentioned earlier talking about capacity building, international corporations, building legal frameworks around dealing with some of these challenges

The second one is a local example which is closer to my heart, and this is actually about the stuff I talked about when we were talking about grooming and farming and children being vulnerable online. This is something my colleagues and I, some of them are in the room, we came up with something like this when we realized that we can't be the cyber police for everybody, especially for the children. And one of the things that we did was if you look at the logos below, that is the logos of the broadcasters, the ISPs, the telcos the celcos and everybody involved in the connected ecosystem in Malaysia, coming together and agreeing on one thing.

We all have to get together and work connectively, to make sure at the very least, children are protected online. This is the first step, there are a few more, that we're going to come up with, and you see the 5, 6 key points, these were the things that were coming out of schools. Cyberbulling, kids as young as 12 who are watching porn on their smartphones, violence in school because they see something online that looks kind of cool, they whack the guy. When do law enforcement people get involved, it becomes a police case, somebody gets knocked on the head. Racial abuse, hate, online gaming and addiction, all these things are happening faster than before. There used to be a time where children would never be allowed in a pub or a bar, not until you're at least 18, or into a gambling den at least till you're 18. But you know now any kid can stumble on a gambling site online and think it's just a game, and this is creating another problem. And then there's the online fraud and deception. So what we did was we got together, the cops, us, industry, and came up with this campaign where we went to all the national newspapers, we took a one whole double page ad nationwide, this is downloadable, printable, it's in every school, every classroom so that kids know about it. And this is one example of how we work in a multi-stakeholder environment. Thank you.

CHAIR

Sharil thank you very much, I'm going to leave questions to be allowed for late when the other speakers have made their presentation. I think we're gathering some kind of mosaic or a map, and there are some pieces of the puzzle. I call upon Hong Xue to help and elaborate more and views on this topic of international law enforcement. Hong Xue is the professor of law and the director of the Institute of Internet Policy and Law at the Beijing Normal University. Seems that we have crossed paths several times before, but we only got a chance to meet yesterday when we were talking about this session, so with you Hong Xue, and I've been told that they are 6 viewers who have been listening on the livestream, so those viewers feel free to ask questions and participate as well. Thank you.

Hong Xue

Thank you Pablo the chair, thank you Sharil. It was a wonderful introduction and very insightful analysis. Especially this is a real law enforcement officer, a man with a gun, (Sharil: I don't carry a gun) oh okay, you carry wisdom for us to learn. And I'm going to present a small perspective, and as Sharil has very insightfully presented to us, there are different levels for law enforcement, and perhaps at some levels there's no law available now, to my rough understanding. I tried to absorb the knowledge I learned from Sharil "impromptuly." The first level maybe we call it cyber violations, including infringement of civil rights, property rights, privacy rights, and cyberbullying happening among kids, and cyber threats. It could be among kids or among grown-ups. For the first level, this is the issue we want to talk about today. And second level is cyber security issues especially about cyber-crime, I guess think is also an issue for us to think about today.

For cybercrime, Sharil has mentioned many many times, such as phishing, farming and hacking, and a variety of forms. For the third level, I guess it hasn't been able to attract much attention, but it's very important we call it cyber peace. It's actually more important than cyber security, if security is only about criminals, and criminals are the enemy of all human beings in whatever jurisdiction they should be prosecuted, penalized. But cyber peace is a critical issue especially we see many big countries are now preparing for cyber wars, there are new armouries in cyberspace it's very dangerous. And the United States recently released its international strategy for internet governance, and it was released at the EGA forum, these are big stakes.

Following that we see the pentagon is going to release a new report on cyber war. I saw many people and many countries are really watching that, what will happen. Especially a summary of the report, we haven't seen the report per se, but in a summary of the report, the United States literally stated that if they were attacked in cyber space, if there are cyberattacks on them, they will retaliate in normal methods. This is very dangerous, it's saying it's a kind of declaration on cyber war, But at this level there is no international convention unfortunately available right now, so maybe that's another area

we could think about, the law enforcement especially the peace of the world is the top priority of the whole globe.

Of course I'm not going to address certain levels, basically the first 2, of cyber violations and cyber security. My perspective is to look at something in the middle, between law enforcement agencies and offences, that's what we call intermediaries, but intermediaries can be in any form, not only on the internet, but we are not limited to the internet intermediaries. But in a very beneath level for the resolution, for the operation of the internet, why you can connect your computer to the internet, why you can communicate with each other, go to the resource level, is covering the internet protocol. IP address, domain name system, when you really think about it, there could be even an intermediary with its back to law enforcement. But now it's becoming more actually. For example the new Project IT Act in the Unitied States, they are using the domain name system to enforce copyright. That's a very interesting initiative. Of course we can see much access provided to provide connections, routing services, storage and hosting services, is of course a virtual hosting server system, and locations are changing, we know the very powerful Google, and linking services. You may think about those map 2.0 services, the new social media, the Facebook, Twitter. They are actually a combination of these categories. You can't really say Facebook is a storage of hosting services, it also has a kind of locating and linking services. And of course Bittorrent and peer-to-peer file sharing system, they are all intermediaries, what they are doing is to link up the people, then provide services to enable you to communicate with each other. And of course they can all be used for law enforcements, the agencies can use then to enforce the law. Especially to enforce against offences, so this is something I want to present on this perspective. We look at intermediaries and what they can do. So what kind of law to enforce, Sharil is very right, he very wisely mentioned in some areas that the law is missing, if there is no law on a legal basis it's hard to enforce.

If law is available, there are actually in 3 levels, this is my understanding I could be wrong. A domestic level, the most famous one, the one that is being implemented in France and UK the 3 strike action against repeated copyright infringers. This is a kind of

fundamental action against these copyright infringers. This means that if you were warned twice for copyright infringement and you do it for the third time, your internet connection could be cut.

In Asia Pacific region, a couple of countries have already implemented the 3 strikes. For example in Korea, I wonder if we have colleagues here. To implement the three strikes, the law enforcement agencies would have to work with intermediaries, the service providers, otherwise how to cut the connection? So it is the internet access provider who help the agency to cut the user's internet connection. This is the ways to use the intermediaries to enforce copyright law, but is this really justified? You copied something on the internet and you lost the whole internet connection, which means you cannot access the e-government services, you can't access e-banking. There's really a big pressure issue in such an internet world.

Well that's one example. I know other countries think about the 3 strikes to use the intermediaries to reinforce copyright such as New Zealand. But there is strong opposition against this kind of all-reaching enforcement measure. This is domestic law, another level we can say is international level, actually in many international laws we can also see this kind of intermediary-assisted enforcement. Dating back to WTO, World Trade Organization's trades agreement, there is an obligation imposed on this intermediaries, they are supposed to provide information for the copyright piracy and trademark counterfeit they discover, these kind of offences, they're supposed to provide information, and this kind of information provision obligation has been extended in the new treaty in the counterfeit trade agreement, the ACTA. Yesterday we have a panel exactly on this. So this is actually on an international level, they also impose an obligation on intermediaries to help agencies to enforce the law.

And the third level , maybe it's not a real level because it's not real laws, these are the kinds of private regulation system, such as from tomorrow we're going to have a weeklong ICANN meeting. ICANN is not an international lawmaking body, it's not a treaty organization, but they keep making many policies. The policies are implemented

by the DNS on the internet. And this from the implementation perspective, they are really binding, they are bound, the service providers are bounded by these policies. So I guess this is kind of global governances, this is created a kind of global bylaw. So these 3 levels of things that could impose obligation on intermediaries and enforcement. Okay, and what to enforce, what subject? Sharil has already given us a crop of wonderful insightful analyses, from what I can see, and this very roughly, and quite short, First, it's about property, copyright and trademark specifically. For copyright I mentioned a couple of times on 3 strikes, and so trademarks, the most famous one is ICANN's new GTL new trademark measures. They are all implemented through these intermediaries, and criminal law for cybercrimes. We have please, well there's real law enforcement agencies, but intermediaries can help to investigate the crimes. Oh the sad thing is what I borrowed from ICANN is called MoPo which means "morality and public order."

In many many countries, this is a big issue. Well I won't use the word censorship directly, because it's broader than that. It's very possible, you are a service provider, you receive a request from a certain government to remove certain content from your system. I guess Google has maintained a very good list and database, the kind of request they received, from which government and on what thing. And some governments warned Goggle not to publish this kind of request. So this is interesting law enforcement, and especially in a cross border context, why Google which is a company registered in the United States received demands from a pacific island country asked to remove a video from YouTube.

This is very much interesting law enforcement all across the border. Another subject could be privacy and data protection, and Sharil mentioned that as well. The others could include a writ of reputation, I've seen some interesting cases against intermediaries for not timely removing the alert defamatory messages or information. For these things I guess it's a little of difficult for the service provider or intermediaries to enforce before receiving the warnings from the right owners, it's very hard for service providers to know this is defamatory. They don't know whether it's really true or it's

wrong, so this is subject for enforcement . And who to do that? Of course I just now claimed the law enforcement agency, they can do that, and now they are using intermediaries to do that.

For this slide, I leveled the 3 layers of internet, according to my research. And very below, I call it the resource level, this is about the normal operation of the internet, so what is working is the RARs, registries, registrars, they are taking care of the technical part of internet transmission to ensure that in operability, the internet domain names can be resolved to the proper places. Normally we don't believe these kind of layers are relevant to really relevant to law enforcement, what is really relevant is the application level such as the social media like Twitter Facebook, the search engines like Google Baidu, the huge data centre services. Actually now not only on the application level but also the resource levels have been involved in law enforcement, so actually this kind of intermediary enforcement is expanding, not only at application level but it's going down into the resource level. What if intermediaries refuse to help to enforce, it refuses to fulfill its obligation of enforcement? There could be two consequences in two different models, one is the liability model. Actually this is interesting, a Chinese provision against intermediaries, if the intermediary refuses to remove the alleged infringing materials, the intermediaries will be jointly liable with offenders.

This is very interesting, so if you refuse to fulfill the enforcement obligation, you are liable yourself directly, this is one model. In many countries, this intermediary liability has a safe harbour to help shield the service provider from the very heavy burden of the risk of liability. But the same harbor means you have to satisfy certain conditions, you have to cooperate with law enforcement agencies or with rights holders, otherwise you will be liable, such as the famous notice and take down cases. If you notified by a copyright owner that is infringement happening in your system you to take down the alleged infringing material. That's kind of a safe harbor, but the consequence of the safe harbor is that this will probably result in a kind of self-censorship. In order to prove my innocence, I never know, I didn't know what was happening, I have my own policy to discipline my system.

Another model is called obligation model, such as for 3 strikes According to UK Digital Economy Act 2010, if a service provider has been warned by the law agency twice that a user has been infringing and for the third time the service will be cut, refuses to cut, they will be subject to fines, so they will be punished with an administrative penalty. So they will be they have to fulfill the obligation to provide the information to authorities, to assist the authorities to do investigations against offences, and of course to take the required enforcement measure required by the authorities, so these two models
This is a brief overlook of what is happening right now, we see different subjects based on different laws, through different levels and there are consequences for not helping to enforce. If is this right or wrong, this is a governance forum, so descriptive does not really help, let's try to be analytical. I want to borrow Mr Frank La Rue the special rapporteur of the UN on human right issues; I guess Frank's report is very insightful. First of all he quoted three principles for law enforcement in cyberspace. Firstly, there is a duty of county, duty of state, all the countries have an obligation to provide human rights, and secondly there is a corporate responsibility to respect human rights norms, so even though you're a full profit entity it does not mean you can only be money oriented, you have social responsibility to respect human rights. So this brings one issue, I know for some big service providers such as Goggle, Yahoo, Microsoft, they operate in certain jurisdictions and they are subject to considerable pressures in that jurisdiction to submit their user's information to authority, for certain legal proceedings, investigations or prosecutions, some of them comply, some of them didn't. This is now a real dilemma for these business, they want to operate in this jurisdiction , in this country, but the other hand that have international human rights obligations to observe, so this is an issue of choice whether they want to sacrifice certain commercial interests to respect international human rights law, so it's a big thing.

Thirdly is that these enforcements through intermediaries is kind of a private enforcement, if I can put it this way. Sometimes this can deprive people's legal remedy, this is really not justified, I know the initial draft of Sarkozy's three strike law does not grant people's right to legal proceedings or a judicial review, means administrative level

can decide to cut people internet connection they cannot say to the court. That's really unfair. So these 3 principles I guess should be respected by all names, And lastly, this is the last thing I want to talk about, if intermediaries must be involved in enforcement, what should be done, this is also very much learnt from the report of the special rapporteur of human rights. First of all, no censorship measure should be implemented through intermediaries. They don't have the proper resources and they may not have the proper acknowledgement to do this. If they are forced to do this, most probably it will resort in unnecessary damage to free speech and other human rights violations. And second there are some multi-stakeholder initiatives such as GNI, Global Network Initiative, this kind of intermediaries on the internet, the big ones, Google, Yahoo, they get together to set up a set of principles on what kind of enforcement they can hold, such as for child pornography, this kind of information should be removed immediately, and what kind of enforcement they shouldn't help, because it will violate basic human rights principles.

The last but not the least is that those intermediaries, the corporations involved in law enforcement, they should have a clear standard and terms of services set up according to international human rights principles. So, okay, thank you very much.

CHAIR

Thank you very much Hong Xue. If it's okay with all of you, I will let Jordan speak and then we can generate a debate. I think we have the perspective from a law enforcement agent, from an academic, Jordan is a policy advisor for the internet in New Zealand and can add a bit of an additional perspective to this mosaic of angles through which we can see internet law enforcement.

Jordan Carter

Thanks Pablo, and good, almost afternoon, 3 minutes to go I'm glad you're all awake and alive. My presentation will be a little bit different. I'm not a law enforcement official, I never have been and I never want to be, nice as such people are. I'm coming from an incident and NZ perspective which values an open and uncaptioned Internet. And the

case I want to talk about is recent changes to copyright law in New Zealand. So that's kind of what I'll do, I'll just quickly say who we are, talk about the context for these changes in copyright enforcement, and look at some legislative screw-ups and then attempts to repair these that have happened in the New Zealand jurisdiction in the last couple of years, and then say a few words about enforcement, because what we're mainly talking about is civil enforcement, not criminal, and so generally speaking, law enforcement agencies aren't around,

Internet NZ is an NGO that exists to protect the Internet for New Zealand. Anyone can join, you can join on our website if you'd like to support us. And we get most funding through the operation of the NZ CC TDL, which is operated through some of the subsidiaries that we hold. And I guess the context for this copyright enforcement discussion is this.. I don't really know where to start, but we have this kind of paranoia on the part of people who create intellectual property and that any copying is cheating them of something, is stealing something, is depriving them of income and revenue that they are otherwise entitled to do so. And that's been throughout the history of copying devices and so you had the dramas at the end of the 19th century when player pianos were introduced, and you had the destruction of the music industry that was going to be created by the rise of radio. And then when records came along, you had a little crisis about that. When the audio cassette was introduced, the world was going to end. When the video cassette was introduced, the MPA and the United States said that this was going to lead to the destruction forever of the American movie industry.

And in the New Zealand case, in the mid-2000s, when applications like peer-to-peer file sharing was playing out, we're all told again and again that the end of the music and movie industry was nigh. Just because of this amazing copying machine called the Internet. The fact that it would suddenly become easy, and to make perfect replicas of digital artifacts, and to share them without paying for them. Now, I don't know if you've noticed, but there is still a music industry. There is still a movie industry. They seem to be making quite a lot of money releasing quite a lot of albums, quite a lot of movies. And so, to me one of the most deeply troubling things about the private enforcement

copyright law is that we constantly see these pushes for tighter enforcement of rights and growing, if you like, exclusivity of rights on the part of rights holders. Responding to a ‘problem’, in quote marks, that doesn’t exist. You can always point to a particular person who might have bought a DVD but instead illegally downloaded a movie, and you could always try and characterize that as lost revenue, but what you can’t point to is the systemic decline in content producing industries. And the only studies that show it seems to have been funded by those industries. And whether it’s the US GAO, or other sort of less authoritative sources, no one has been able to show you have evidence of economic harm from the fact that more and more content is available to more and more people, than just everything before.

But we do face this global question, this type of enforcement that hasn’t changed in recent times and it isn’t going to change, because that was discussed at the panel yesterday. Powerful countries acting in their own interests. And we’ve got a country in the US that is powerful and able to act to persuade other states to tighten intellectual property laws and they have a view that doing so is in their economic interest. So that push isn’t going to go away. We’ve seen that the global multi-lateral institutions like the World Trade Organization and the World Intellectual Property Organization, are not delivering, quote-on-quote, for those who would like to see sharply tighter restrictions.

And so we’ve seen a leakage of these policy debates into what we’re horribly calling plurilateral negotiations, the anti-counterfeiting is one example of a chance at a partnership is one bilateral trade agreement that has been discussed elsewhere, where negotiating countries agree much more intensive regulations of intellectual property law than national jurisdictions might otherwise choose. And of course this global policy debate gets pressure from the US and has affected the New Zealand policy debate. The New Zealand government, for reasons I won’t go into here, but mainly do the dominance of agriculture deal with the economy and all these export industries has always sought market access openings in developed countries, to get access to agriculture markets. And one of the holy grails of New Zealand trade policy is the free trade agreement with the United States. This sets up an interesting dilemma for the

country in terms of.. we want access to sell meat products, dairy products, and culture products to you, and you want us to rigorously enforce IP rights. Is this a trade that we would like to make? That's a context that I'll come back to later.

In New Zealand we have a copyright act that was completely re-written in '94 and enforced in the usual commonwealth style of setting up broad rights for cradles of intellectual property and then having particular exceptions to those rights that allow people to do things. We signed the TRIPs Agreement again in the mid-90s but we didn't join any of the WIPO Internet treaties. And the New Zealand government's point of view has been that IP law should be struck in the public interest of New Zealanders. And as an IP importing country, generally speaking, the view has been that massive tightening of such laws is not in our national interest.

But the act of '94, '94 was the mass uptake of the Internet, so the government decided that they were going to have a look at the technology neutrality and suitability of the acting of exceptions. And it took them 6 years to do this review, which was quite a slow review, I think, by anyone's likes. But they came up with some good things and one very bad thing. And they added an exception for format shifting. Before they did that, in theory it was illegal to copy a CD that you want to put it on your ipod, and the government did realize after a while that with everyone's doing this kind of thing including Members of the Parliament, and officials that might be good to get into law and exemptions that allow people to do it, and there was recognition that Internet service providers as intermediaries should have some protection from liability that they aren't responsibly necessarily for their users do and so some safe harbours were created in the act, which kind of felt somewhat, or should I say, foiled. And a new section was added that if a content host was notified of infringing material being sought on their service, they will be protected from liability if they remove it. We weren't too happy with this because of the chilling effect it potentially has. For a nice piece confronted by an allegation of something being infringing material, and they have any doubts about whether it might be or not, it might be safe if they delete it or block access to it, but they expose themselves to liability if they don't, we hope that balance is wrong.

And this became known in New Zealand in Section 92A, a clause for which I've put the exact wording up there." An ISP must adopt and reasonably implement a policy that provides for termination in appropriate circumstances of the account with the internet service provider of a repeat infringer." And a repeat infringer was defined as someone who actively infringed copyright, in a way.

So you must adopt a reasonable policy, that provides information in appropriate circumstances, but the law didn't define any of these things. And the government of the day, their stated expectation was that the ISP is in the right, representatives can negotiate about how to implement thos, which left us scratching out heads, but of course if they didn't have this policy reasonably implemented, whatever that meant, they would be exposed to liabilities as intermediaries, they would not caught by the same partner. And unsurprisingly, the ISP and the rights holders couldn't come to an agreement about how to enforce this. There was an election in the middle of that negotiation process when the new government came in that hadn't been particularly in favor of this approach.

A large campaign called "Black Out" was organized by the local Internet community that saw enough mainstream media pressure that the government suspended the limitation in that clause, and then agreed to do a complete review, which took another two years. And hence all of this is, the case here is infringing file sharing. The intended target of this legislation is peer-to-peer. And now we can have an argument on whether that's relevant anymore, whether the p2p infringing is already declining or not but we'll just leave that aside. So what this system does is kind of replace where they thought they might go in the negotiation about how to reasonably implement the policy. It's codified in many pages of legislation. And basically it's a notice system, where if you're caught infringing by a rights holder, they can send notice to the ISP and the ISP can support to notice the customer. If it is a second infringement they can get a different notice, if it is a third infringement they get a different notice. And at that point, rights holder can trigger a process in the New Zealand copyright tribunal, which until now has been a body to deal with licensing disputes and serve maybe two or three cases a year. And suddenly it's

going to get a lot busier at the taxpayer's expense. So one of the features here is that the law provides a strict liability of the account holders. There is no defence, as if the account holder was to say, "oh a friend came over to use my WIFI and downloaded this material." That's not a defence. There's not defence also when an open WIFI port or for your WIFI to have been hacked, none of these are considered acceptable defences under the legislation. And when the third strike has happened, the copyright tribunal can deal with things on the papers without representation. And hence the way they act is not quite as bad as initially drafted but it looks like if the account holder doesn't challenge a notice, the copyright tribunal is entitled to treat that notice as private facing evidence of infringement. So with that the account holder doesn't respond at all, and there are three infringements, then the tribunal is entitled to assume they are guilty. And the maximum penalty you can imposed is 15 thousand New Zealand dollars, which his around 12 thousand US dollars.

Now there isn't yet a formula for how such penalties will be awarded and this is of some concern because this regime is set to come in on 1st September, and it was only passed by parliament in May, so it's all quite rushed. And the worse feature is that the government also included in the legislation a clause that is not active today but could be made active, that gives the district court the power to impose an account suspension for repeat infringers, for up to 6 months. While that isn't active now, the dialogue in the parliamentary on the passing of this legislation indicated that if they regime does not work, whatever that means, whoever measures that, the stricter penalty of account suspension by the District court will be introduced.

So that's the legislative position, I guess the point to make is that all of this is privately enforced and this is all civil law. What we know is that the rights holders in New Zealand uses some kind of detection net to monitor infringing on peer to peer networks. Probably no thanks to Wikileaks is that the US chief provider pays half a million dollars of funding to establish this system, which was not welcomed in New Zealand when it emerged earlier this year. What is good from our point of view is that instead of that previous little clause which would have basically made ISPs, judge jury and executioner would have

had people's accounts being terminated left, right and centre just to protect the ISPs from liability. We now we have a perfectly accountable judicial process in an administrative tribunal that at least means that there is a chance for a proper hearing of the evidence. And so ISPs do protect their services conduits and the other thing we don't know is what the volume of notices will be. That will entirely depend on the fee that is set for launching notices, the right holders are arguing for a few cents per notice, the ISPs are arguing for 50 dollars a notice, and obviously there's quite a big difference in marginal costs for the enforcement efforts. But that is one of the challenges that we face If there is another election this year, if there is a change of government, then one of the issues that the NZers have to fight is how do we decide whether this regime is working or not, because we do not have any confidence that the rights holders are a reliable source of evidence about levels of infringements, and we don't believe that the number of notices launched is an acceptable measure of infringing either, but we don't seem to have any willingness yet on the part of officials to create or fund some independent research to actually try to ascertain the level of that. And we have as usual in this debate, completely left behind the actions of stating the issue of is this a problem that needs to be fixed by public action or not, is there a major economic hind is there a big problem. And divine notices will be an issue if small ISP there will be funded by thousand of notices, that's going to be a real problem. And we don't know how severe the tribunal will be in terms of willing penalties.

We don't yet know the implications of the transcript partnership negotiations which speculatively not going to be finished this year, but which may end up with tightening the requirements that go beyond this legislation. And we have this constant pressure to be constantly be typing these laws, so everything's that done, then leads to further complaints, on no infringing is still going on, you got to tighten the law to protect us. From my bit it would be nice for them to see a serious shift of the goalpost in the other direction or at least an acceptance by rights holders that they've gotten as far as they're going to get, and the settlement is fixed, and they're not going add anymore pressure to tighten this laws further, in the absence of evidence, objective, reasonable evidence that probably needs to be fixed. I hope that was of some use to you, thank you.

CHAIR

Wow, I think we have a lot of material for discussion. I would like to open the floor up for questions to ask the other panelists to engage in. I think we have deeper levels of the elephant of international law enforcement and this could generate a very good 15 minutes that we have left to engage in a dialogue. Anyone on the floor would like to take the microphone?

FLOOR

(Louise Flynn) Louise from APNIC. We talked across three different speakers and the issue of jurisdiction is quite interesting to me, in this how this seems to be initiatives at the national level regional level and international level. And I want to get some perspectives from you on how the enforcement side of that is going with all the conflicting laws on all the different levels.

REPLY

(Sharil Tarmizi) I think the enforcement side, I assume you are talking about criminal situation or is it a civil situation (Reply: criminal), well it's actually not that much different. Very often what happens is that, again, like in the internet community, the law enforcement community works on the basis of formal and informal.

It's usually easier when you know the guy on the other side that you need assistance from, especially when you trace something and it pops up from the other side of the border. However the challenge is when sometimes you do that without usuing formal, legal avenues, the evidence that you have gathered is not admissible. So if you come to a point when you want to prosecute the guy, and say okay, we tracked him and traced him and done this and done that, we can only use it as information, not use it in the prosecution situation. So very often all our cases get chucked out by the court because they say well, you can't prove the link, you can't prove the nexus that this guy did do what you say he did. So it continues to be challenging for law enforcement, especially cross border because going through the process and the procedure, although

necessary, takes time. You need to go through, you know how governments are architecture, it's law enforcement agency, foreign affairs ministry, then maybe another ministry in between that, then at some point it goes out, in a treaty, when you apply for mutual recognition of that. It becomes more complicated when you have situations where such an offence is an offence in one country but not in another country. That you tend to get in cases which are, I think to use an example, the quasi-area, the sort of in betweeners. The guy will say look, fine, he's sitting in that country, I know where he is but I can't do anything about it because actually it's not an offence. Where do you go?

These are again some of the challenges, the jury is still out as to what can be done about it. I know that at the UN level, there's an initiative by the UN central working group to try at least solve consumer issues relating to enforcement when it comes to transactional stuff, e-commerce. So there's a working group now working on online disputes resolution and e-commerce. That's different from the UN central model law right now, that's a little bit further on. So I hope that helps.

I was just going to ask: how many of you feel that downloading music is right or wrong? Okay, how many say that downloading music without paying the artiste some money is okay? Okay I've got 3 or 4, 5, 6. And how many think that that's not fair on the artist and something actually needs to be done on it. Which side are you on Izumi? Although it looks like a philosophical debate, I think you would have seen in the recent year or so, and in the other presentation, governments are increasingly under pressure to sort of enforce intellectual property rights, and it becomes a nightmare when you try to do it online. I mean you can deal with bootleg CDs, when I say bootleg I mean pirated CDs, DVDs, that's one thing, but when you're doing it online on a server, it's one location and it's situated the other one is on a secondary server somewhere, it becomes a problem. And yet there's some people who feel that, no, there are kids, younger kids, who won't understand the version of intellectual property rights, they will say "what's wrong with downloading music from Limewire?" Now I'm just wondering what's the sense, because I know that there is the creative commons approach of looking at intellectual property rights and there's the traditional one.

(Jordan Carter) It's quite a difficult one, I mean I don't condone breaking the law, but I break the law sometimes. So I don't anymore actually because I now got an iTunes account and if I want to get something I just buy it on that because I am able to afford to do so. But a number of years ago, I'll be of the view of if I heard of a song if I wanted to hear again or someone told me the song was good, before most songs you might want to sample the song on YouTube, you might go on Limewire and download it and listen to it. I only had my Limewire set so that I would download things, I wouldn't upload anything, but if I'd like it I'll go buy the CD and delete the track. So I was infringing copyright, and the economic effect of my infringement was to increase the revenue to the artiste, but that was the way I chose to do it. If I like that track, if I had friends who listened to music, I'll of course give them some money, so that kind of thing. But I think this also it doesn't help necessarily to individualize it like that. If you think of it on a broad level, we've had an era of big music, if you like, as an example, with bands like REM or U2 would go and make hundreds and millions of dollars and have millions and millions of fans all based on a kind of industrial Euro model of big marketing and expensive things. And that was built on a control and distribution that was built on the fact that they could sell records and sell CDs for $30 bucks and sell millions and millions of advertising and get sales and results. A pre-internet world, and now we've got internet and the world is different. And so maybe in 50 years there won't be mega-bands, if there are mega bands it will be because they were famous through social networking sites. And we have a situation where there are many more bands that are making a little bit of money, but where music, which is a fundamental part of human culture, plays a less significant economic role than it has done. Who cares? I don't care. I listen to music because I like music, not because it's an industry I wish to support with my dollars, and that is just the many many things this fantastic revolutionary thing called the internet may cause. And I'm not here to explore the past, I'm here to explore the future.

CHAIR

This is fantastic, actually for the sake of the record, When Sharil asked for those that were okay by downloading music without paying, many raised their hands. And actually the same that raised their hands, also raised it when they agreed that the artistes should be compensated for their music, so that's for the sake of the record if you didn't see it in the webcast. So I would like to know if those that raised their hands would like to say something or speak a little bit more about their argument. I think this is a fascinating discussion.

FLOOR

(Izumi Aizu) Well we are living in a very complicated world, I believe that sometimes you are the producer of music, sometimes you are the consumer, sometimes you are the intermediary sometimes you are the policy making, law enforcement, in the same hat, in the same person. And some people are pretty poor, others are very rich. And as you mentioned the business model of distributing music, has become sort of obsolete on one hand, but at the same time if you're a poor musician and you want to make a career and want to make some good money, there should be some justice, and we're all struggling where the solution is, that's why I raise both of my hands. Both seemingly are right but somehow it doesn't really work with this technology, it doesn't mean that you create a new platform after say iTunes. So the flat rate solution is one thing, but the flat rate of iTunes or the flat rate of all entertainment combined with connectivity and advertisement, so you pay $20 for an unlimited use of unlimited anything, and that money may go back to the musicians if they are very popular? I don't know, I don't have the answer right off, but there should be some creative solutions combined with technology and social systems. That's where we're struggling for other than just penalizing the unfortunate guys.

(Louise Flynn) I'll speak as Louise Flynn the individual, not Louise Flynn from the organization I work for. I'm from a marketing background so I'll say this as a commercial issue. In my study of marketing, some of the more recent marketing study is about disruptive innovation, or innovation that occurs because what is in the market doesn't satifiy a new type of user that behaves differently and I think the music industry and

what has generated through the conflicting issues of people that both respect an artiste and their ability to generate revenue for their talent and the fact that they don't want to participate in the current business model for music leads itself to behaviours that are different. So much like Jordan, people want to try, people want to listen and attempt to buy afterwards, so the misconception that people download content exclusively not to then go out and purchase it themselves is kind of a misnomer, so I wonder if it's more of educating the industry and making them adapt to these new trends.

(Unknown) Thank you. I think to me as a producer and consumer of both side of music, I think the issue is more to me all the variables raised are correct, but could we also add a way of, perhaps belittling, or making the music industry less powerful? I think to me that's where the problem is. So if I were a busker at the train station and the consumer who likes my music gives me $1, there is no intermediary, basically it's between me, the producer and the consumer. But when you have a huge industry that we really don't know how much value they add, except making nice CD covers and what else, and they take a big chunk of the product's revenue. I think that's to me where I see the problem is, so thank you.

CHAIR

Thank you very much, unfortunately we're running out of time and I would like to thank everybody for joining this debate and let's continue this debate on twitter for example, following the hashtag "APRIGF", and it started well and hopefully it can continue. Also there is lunch now, so let's seat together if you want to continue the discussion.

EMCEE

Thank you Mr Pablo Hinojosa. Now let us welcome Ms Yvonne Lim who has been working very hard in these few days to present a token as an appreciation to our Chair, Mr Pablo Hinojosa, let's welcome (him).