FINISHED FILE

ASIA PACIFIC REGION INTERNET GOVERNANCE FORUM
TAIPEI 2016
A NEW INTERNET ERA

26 JULY 2016
TAIPEI ROOM 402 (C+D)
WS 2
REGIONAL TRANSPARENCY REPORT AND
ONLINE RIGHTS PROTECTION MEASURES

Services provided by:
Caption First, Inc.
P.O. Box 3066
Monument, CO 80132
800-825-5234
www.captionfirst.com

***

***

>> EELING CHIU: Hello. Could afternoon ladies and gentlemen. I'm Eeling Chiu, the Secretary-General of The Association for Human Rights. Thank you everyone for participating on the panel. Also, this is my honor here to moderate the panel, Regional Transparency Report and Online Rights Protection Measures. Today we have a lot of great speakers from different countries. We'd love to hear from them about their findings and difficulties on the topic.

From 2010 Google announced the first transparency reporting award. After it was known event, so far there are more than 60 corporations and organisations that release their Transparency Report.

Among this report, some were especially focused on the government's statistics and request the government to expose the related information and seek a more open and transparent government. Different from the corporate transparency report, this report is usually produced by the civil societies.

Today we have Hong Kong Transparency Report which is organized by the Media Research Center in Hong Kong University. Benjamin Zhou is in charge of the project and Hong Kong released the first government Transparency Report in 2013 and their report has become a very important reference for other countries.

And also Korean Internet Transparency Report is managed by the

education center. And Mrs. Jiwon Sohn, with assistance of (?), is in charge of report and finished the second report last year. The Taiwan Transparency Report is by Association of Human Rights. And Mr. MingSyuan Ho is in charge of the report. Today we have some printed versions here if you need one and can come to have one.

China, Mr. Clement Chen, the postdoctoral (?) of faculty floor in Hong Kong University, and he's the expert in the transparency issues on the PRC government. Although there are no transparency report in China, but Clement will introduce us about the surveillance and censorship in China.

So now maybe we just start from the first speaker from Hong Kong, and each of you will have 10 minutes to present. And after that we will have a 20 minutes for discussion.

>> BENJAMIN ZHOU: Test. Thanks. Good afternoon, ladies and gentlemen, I'm Benjamin Zhou from Hong Kong Transparency Report. Welcome to join us. I'm going to introduce the Hong Kong Transparency Report. We are going to -- we published the first report in 2014 and we are going to publish the second report in 2016. So let me introduce what is Hong Kong Transparency Report. Hong Kong Transparency Report is a Transparency Report basically focused on how the Hong Kong Government obtained and used the information and asked the Internet Service Providers to remove some consent, like most of the Corporate Transparency Reports like Google, Facebook, Twitter, but we focus on the government information. So as I said, we were published in 2013 and published the first report in 2014, and we're going to publish the next report.

So today here I'm introducing our 2014 report. It's just executive summary. So first the resources. We obtain the information from two resources. First, it's from the government release, but in Hong Kong there is no routine releasing about this information so we worked with the lawmaker, Charles Mort with questions by the legislative council for 2013. So for the Hong Kong Transparency Reports, our reward is basically draft questions with reference to the other Government Transparency Reports and the Corporation Transparency Reports.

You can see there is a table there. That's our questions. We list what we want to know from the governments and ask the government to reply. Fortunately, the Hong Kong Government reply most of the information.

The second is that we send inquiry to the Hong Kong government, this is information law, and fortunately there were lots of companies' reports and they received requests from the Hong Kong Government. So there are -- so far there are seven international companies. Unfortunately, no Hong Kong company reports such data so far.

Sorry. Yeah. Google, Microsoft, Twitter, Apple, Facebook, Verizon.

So let's go to the data. Here we have the data from 2011 to 2015. So the first chart you see is the use data requests. It accounts for

92% of the government -- the Hong Kong Government request to the service providers. You will see basically the request is from the Hong Kong Police. And for the constant removal request is basically from the Department of Health because they asked the service providers to remove the illegal sales website. So overall, basically police is the major requester.

So let me see the trend. I think there is good things in up to 2013 that the Hong Kong Government send less requests in particular to the seven service providers which has published Transparency Reports so far. We know 2013 is the average northern -- and why the Hong Kong Government sent less requests? I have another finding. So we see that the service providers, the seven service provider, Google, Facebook, Twitter, in general they reject 40% of the use data requests from the Hong Kong Government. So the Hong Kong Government may be more cautious when they send requests.

Fortunately, Google released some anecdote about how it handled the request from Hong Kong Government. If the government sends, for example, without court order, for example if the information is incomplete, they reject.

And there is another challenge that -- this data is from Facebook. We see that there is a significant rise in 2015 to the request to Facebook. One issue is because in the late 2014 there was an Occupy Central Movement happening in Hong Kong. It was a mass protest asking for -- universal suffrage in Hong Kong. So after the protests there is arrests. 60 people -- 16 people have been arrested for their speech for violence -- yeah. The police send more requests to the social media platforms.

And so issues. First, the government -- we sent requests -- we sent inquiry to the government to ask about the data about how many requests is accepted by the service providers, but police force rejected to review such information and as well as the revenue departments. So we don't know how -- we don't know such data from the government.

So as you'll see now -- sorry. 40% -- this data is from the service providers. And second, the police also reject to review how many requests was sent with court order. I think it's a basic issue. According to the law in Hong Kong, the government bear no responsibility to use a data request with a court order. But we know a lot of international company has a policy requiring that the government send with court order. But the local company that has no such policy.

So another issue is that there is a lot of guidelines inside the government departments, too, about how to handle the requests, how to send requests, how to review such information. That's another issue in Hong Kong Government.

So improvement, we start to send such -- we start to ask that information from the government in 2013. Fortunately, we have more and more information on that, and I think the Hong Kong Government has done a good job. Most of the information we inquired, they responded

properly.

And we raised recommendations for the Hong Kong Government. First, set an independent review of request practice. And second, we establish and make public the internal guidelines. And third, make public the release of the information on the government requests. We also recommend local corporate -- local service providers to release Transparency Reports because it's not just about the government.

I think in Hong Kong -- Jiwon and MingSyuan are going to discuss the situation in Korea and Taiwan. Compared to these two jurisdictions, the issue in Hong Kong is that Hong Kong is not -- and we have a comparatively weak civil society. So the public awareness is an important issue to accept pressure on the government in terms of the transparency and privacy protections and freedom of expression.

So from last years, lots of initiatives from the civil society starts. For example, you see there was a rating project called Who Is On Your Side, rating the local companies, their performance over how they protect our privacy, and how to protect our freedom of expression against the government. And there is two initiative released this year. One is the Access My Info, helped citizens to obtain information from the telecommunication companies. This is important because it raised our awareness about our privacy issues. And second is the Internet Freedom Manifesto. And in particular, after the 2014 protests, the rising of civil society puts more pressure on the Hong Kong Government.

Okay. Thank you.

(Applause)

>> JIWON SOHN: Hello. I'm Jiwon Sohn, the Project Manager of Transparency Reporting which is analyzing the data of South Korean Government Internet Censorship and Surveillance. Transparency Report on national level is of high importance because it informs the public about national level of Internet freedom. And this is especially important in a country with an authoritarian system where the government's request of surveillance or censorship is a de facto binding effect on the corporation resulting in a long-arm reach of the government power. So the companies hardly have room for discretion.

First, I would like to introduce the current status of Internet censorship and surveillance and its transparency in South Korea. In South Korea a total population of about 50 million, about 100,000 online contents are taken down yearly by an administrative body, KCSC, Korean Communications Standard Commission.

On the issue of Internet surveillance, each year about 2,000 accounts are intercepted and communication -- metadata of about 200,000 accounts, and subscriber identifying information of about 600,000 accounts, was provided to the law enforcement agencies.

The number of search and seizure from the communications service provider which can require all kind of communication data is not disclosed, but we roughly estimate it at over 3 million accounts were

surveilled during the search and seizure based on Transparency Report of two major OSPs. This is for the Internet only if you include the figures of all sorts of communication. The numbers are going to be much longer with about 10 million accounts, almost 20% of total population.

Because the scale of Korean Government Internet censorship and surveillance is so immense, acknowledging the citizens of such a serious and Transparency Reporting on nationally is very necessary.

In regards to the level of Korean Government transparency, for the surveillance, the government discloses the total number -- the total number of interception and the provision of communication metadata and subscriber buying information, which is reported from the local service providers to the government twice a year. There is law which mandates the communication service provider to report to the ministry of ICT about service data -- provided data to the investigative agency.

As I mentioned, the government does not disclose the status of the search and seizure which can collect the whole spectrum of data including the contents, metadata, and subscriber-identifying information.

For the censorship, KCSC discloses take-down request of each quarter by categories and general reasons and publishes a paper tri-annually with more details stated. Also they disclose more specific details upon requests and liberation committee held semi-weekly that can be attended by anyone who applies in advance. And the minutes are loaded regularly on the home page. But we cannot know the entire contents of all individual information because they usually review just a few representative cases for each category or only the problematic part in one information.

I do not believe the government would buy its own initiative, establish better practices in regard to the transparency. When I request the disclosure of more details statistics, they just said they do not manage or store such statistical data. They seem to request on the ground that such disclosure can disturb investigative activities. I think it will only be the resolution which mandates government to disclose more data.

And to raise awareness of the surveillance/censorship of the government and proper evaluation thereof, the disclosure of merely the total number is not sufficient. A more specific and detailed statistics is needed. For surveillance and statistics for suspected crime, durations, surveillance, and rate of indictments must be also disclosed to the public.

Also, more individual cases should come under public scrutiny. In Korea, after the revolution of indiscriminate surveillance on popular mass chat app case, people started paying attention on the massive surveillance and transparency issue. And the company in Korea began publishing their Transparency Report. And recently the campaign

calling for citizens to inquire their mobile service provider, whether they provided the information to agencies is being held. It was discovered that numerous politicians and activists and union activists and journalists were being surveilled. As a result of this revolution of individual case, the public became more aware of and alarmed by the governmental surveillance.

In order to bring this individual case to light, notice to the effected must be strictly given. I feel that the concept of transparency in relation to the communication surveillance and censorship seems to be moving from a unilateral disclosure of the total number by government or corporation to let know whether a person information has been given to that government.

I think this is a positive development in the Transparency Report project's ultimate goal. Yeah. And to find out more about the South Korean status, please visit our website, and thank you.

(Applause).

>> EELING CHIU: Thank you for the presentation from the Hong Kong and Korea. And we think it's very important not only about the transparency but also freedom of speech and privacy issues. So now we'll come to Taiwan Transparency Report, MingSyuan Ho.

>> MINGSYUAN VINCENT HO: Hi, everyone. I'm MingSyuan Ho and responsible for the Transparency Reports and working in Taiwan for Human Rights. So Internet Transparency Report is reported by Taiwan Association for Human Rights and the most in the past were focused on the traditional human right issues, like anti-death penalty, freedom of expression, right to housing, refugee, et cetera. But there is only one exception, at least, and its exception is Taiwan. Taiwan also cares about the personal data protection. The reason it's also passed on the context of national surveillance and that's also a root for us to do Taiwan Internet Transparency Report. We published the report last year so you could download the report from the link. And the TITR or Taiwan Internet Transparency Report is the first project for Taiwan, mainly for the digital human rights and public transparency.

So this -- in this report the data we used, mostly come from government. We try to use the data already released or the data we asked by Freedom of Government Information Law and the above two ways were useless and we were asking legislators for help. Also we can buy some Corporate Transparency Report to finish this report.

So in the past, yeah, in the past Taiwan seldom large scale event on surveillance or censorship. We only had one big event in recent years that happened in September of 2013. And it is Taiwan's Supreme Prosecutor tried to wiretap the Parliament and result to our President. So just this big event. Yes, but I think it doesn't mean that we are safe. Why? Because according to Taiwan judicial statistic, Taiwan's police and department actually over 15,000 communication surveillance every year and this is a rather high density compared to Taiwan's population.

If we compare to United States, you will find that although the number is already quite large, the list median population country just issue about 1,000 to 4,000 warrants every year. So and the second reason why we are is because we also sent over AT request to government last year and we also know the communication surveillance, many other Taiwan government departments also gain some power from different loads to first Internet corporation hand over personal data if it is necessary.

So this formalist -- this formalist, unless it's provided by a different department. And you can see that some department, they are very -- they just tell you to go basically to a website and try to find your information yourself. They don't want to talk specifically. So in the first year, TITR took lots of effort to clarify a list situation. We tried to make government tell the citizens on a legal basis the statistic and extent of operation procedure.

So there is two part for personal data request. Actually for both part, the personal data request and the content removal request, the two part we got is so limited. You can see -- it's a little small, but you can see the largest number is 2,237 for Criminal Investigation Bureau. And, of course, it's incomplete. If you include all communication surveillance mentioned before, you will get a much, much higher.

So -- so in the first year report we have a strong need to integrate and incorporate other public report to supplement our insufficiency. We tried to integrate some corporate Transparency Report like Google, Yahoo, Microsoft and Apple, and tell the citizens our government is very lazy. The data is really ridiculous if you compare to other corporations. Yeah. I think I don't have to mention too much. You can just see.

So for content removal, based on the statistic provided by the government organisation, they had -- they sent 1,234 requests and the successful rate is 91%. But if we check the Google data, we'll find that the successful rate is just above between 0% and 30%. So there is a big gap of compliance rates provided by the government and corporations.

And the other one -- the other problem is that we find that in Taiwan we have -- we have an organisation, semi-official organisation called iWIN and according to their outsourcing operation, it includes administrative technical operation, monitor Internet activity, implementing, but not related to the exercise of public power. So it just got transfer to different government department. But if -- in last year we find that some government department are unclear about iWIN duty and responsibility. Take iWIN as final orchestrater, and I would never clearly introduce them. It's on duty and responsibility on their website. So yeah. That's not a problem.

So we have information is so limited. So why is information so limited? We think the problem seems to happen on the interpretation of freedom of government information law because some government

department tried to tell us that the freedom of government information law could only force government to release the existing data. And the first government could not allow government to make statistical -- however, if we rethink that just a half year ago, the government surprisingly topping the open global data met by foundation. I found that is maybe the reason. We think it's not true. Because open data and freedom of information in Taiwan uses the same law and the open data often organize and create new data format. I mean, government, of course, could make new statistical format. After all, every format should be created first and then it could be open. So open could become impossible if just some sensitive issue were touched.

And so let's talk about some suggestion and improvement. The first of this part is we lack an authority to be responsible for right to privacy on Internet and you will make for deficiency. That is lacking overall policy. And it's hard to proactively investigate whether there is a privacy reason or not. And third, it's easy for government -- to check the data release.

And the last one is operational procedure to send in requests that are different and by each by each -- for each government it's different.

The second one, it is such that we should increase the protection scope of communication surveillance. Because of the communication surveillance law in Taiwan, only regular, heavy is related to telecom. We find that according to official document by Ministry of Justice, once the email content has been stored and then it will not be regulated by the communication surveillance. It will be regulated by code of procedure -- criminal procedure. And Communication Surveillance Law is a more stricter law compared to Code of Criminal Procedure.

And otherwise, we also have no -- we also have no successful -- now. Yeah. So because if you are under surveillance, under communication surveillance, then after the communication surveillance is finished, you will get a notify, and we found that -- cities then tried to appeal. They are under improper communication surveillance, but no one is successful.

So the third one is the local telecom and Internet corporation lacks transparency. And still no local telecom or Internet corporation try to make their first transparency report. This is really important because the transparency report is citizen is accountable. And the customer should know how data and content be treated in corporations' policy.

And if we have some corporate transparency report we also helpless report for Internet Transparency Report to sup advise whether government can or not. So that's all. Thank you.

(Applause).

>> EELING CHIU: Thank you, MingSyuan, for your presentation. According to the statistics, it seems like Hong Kong and Korea is more honest than Taiwan Government. Okay. Then we'll have Clement Chen

about censorship in China.

>> YONGXI CLEMENT CHEN: Compared to statistics described by previous speakers there are no initiatives of Transparency Report yet in China. Given the legislative developments concerning information rise, namely freedom of information and personal data protection, and given the changes in the regulatory approaches of surveillance and censorship on the government, there is some possibility for the Chinese society to introduce Transparency Report on censorship in China. So I'm going give a brief description of the whole picture without going into the details.

There are two legal bases for Chinese citizens to request information considering surveillance on censorship. There is a freedom of censorship regime in China since 2008. Like Hong Kong which has a relatively soft coat to information. China introduces a statutory basis of the right to access of information. Although there are very broad exceptions including but not limited to privacy, trade secrets, there are also some special exemption, for example, information disclosure shall not endanger social stability without a statutory definition of what amounts to social stability.

But it is still remarkable that the Chinese legislature allows citizens to challenge governments, not disclosure of information before the court. So this is rather landmarking when we considered the engrained history of security in China. And according to my statistics, it seems that during the first several years of implementation of the FOI Regime, China is doing quite well in terms of the volumes of information requested by compared to other relatively mature FOI Regimes. You see that the average FOI request per 10,000 -- I'm sorry. 100,000 population, China is doing pretty good. Even better than Canada and Germany and Switzerland. And in terms of the FOI litigation, you can see the line indicates that there is a very steadying increase of FOI litigation during the past seven years which indicates that the Chinese citizens is rather active in asserting their right to information.

Okay. Apart from the FOI Regime, under some recent legislation concerning personal data protection, especially in the legal -- in the field of civil law, Chinese citizens are enjoining the right of access to their personal data held by Internet service providers as well as telecommunications providers. Although in other areas their access right may be rather limited. And even in terms of government-held data under the FOI regime, citizens also are entitled to have access to a certain degree of personal data held by the government. So which introduced the possibility of requesting for their personal data in terms of Internet censorship and surveillance, made those requests with the government.

And, but however there is actually a huge imbalance between the privacy protection, vis-a-vis government agencies with privacy protections vis-a-vis private sectors. Generally speaking, we can

imagine that citizens may have broader right of access to their personal data held by ISPs, where is they have very limited right of access to personal data held by Internet regulatory agencies.

And secondly, although in the old times it seems that we all know that the Chinese Government is having very intensive measures of Internet surveillance and censorship, but it seems that in recent years there is a change of the regulatory approach which is the government is increasingly open with their legal basis of surveillance and censorship. They are now literally making norms and other normative documents with legally binding forces which indicates under which conditions your personal information is detained by ISPs and transfers to the government agencies.

One typical example is the introduction of the real identity registration to almost every aspect of Internet services covering, in this chapter, consider covering from the registry, your subscription to Internet services. Your subscription to telephone services and microblogging, and instant messenger as well as apps in smartphones. And those are regulatory -- under those regulatory regimes, ISPs are under pretty stringent obligations of collect and preservations of real identity information of their users. There is -- it is very unclear to what degree are the government agencies under similar obligations of data protection.

Also, from the part of censorship, there is some significant changes in terms of both the structure of governance as well as legal basis for censorship. Since 2014, Chinese Government formed a new department who is exclusively responsible for so called regulating Internet contents. So it is empowered with extensive authorities in terms ranging from content removals to punishment of those Internet users who have published, so called, harmful information online.

Also, the Ministry of Public Security also publicly declared that they are now introducing the so called Internet policy parole on a daily basis. And the statistics shows that just in four months of last year, the online police has found more than 758,000 pieces of harmful information that violate the law and have finished investigation of 17,000 cases. Which means there are -- in those cases -- cases who got punished.

And you can see from the official website of the Cyberspace Demonstration, there are extensive -- a great number of regulatory documents which regulates the Internet content in relation to almost aspect of Internet services and they are just -- they are also publishing at the ministry punishment decisions regarding content removals and other activities that are considered as in convention of Internet regulations.

So actually there have been some cases of -- in which citizens have filed FOI requests regarding the activities of, censorship as well as surveillance in China. Although all these cases failed, and actually the information requested were eventually detained on other

grounds and it indicates, at least, that there are some very premature, but yet fundamental, channels of access to information regarding Internet censorship and surveillance as well.

So actually there are some minimum legal channels in place, but there is still a long way to go for the civil society to being able to really have access to those information and engage in further activism in terms of influencing the Internet Governance inside China. So that's a very brief presentation, and I look forward to your comments and questions. Thank you very much.

(Applause).

>> EELING CHIU: For our presenters, thanks for the presentation. And we are very sorry as we only want to focus on Northeast Asia because the fact it is only Hong Kong, South Korea and Taiwan has the Government Transparency Report, so it will come that other countries can join our work. So now we'll open the floor and see if anyone has questions for the presenters. The panel will be closed at 1:00. So we have 10 minutes.

>> PAUL WILSON: Hi. I'm Paul Wilson from APNIC. Thanks very much for these. It's been a very interesting workshop. My question is about for Internet reliability. I didn't hear a reference to those. But the Manila Principles seemed to be good at describing from the immediately, the companies actually carrying the data how they're able to carry requests and what their expectation should be with transportation and so on. I'm wondering if the Manila Principles are being considered useful input of this process or actually all well aware of them? Thanks.

>> Hi. Thank you for the presentation. A question on the data that was collected. I was wondering if there is a gender breakdown especially on those that are surveyed, that are under surveillance? What are the percentage of male and females? And also if you have any information on the types of contents that were blocked, that would be good to share because we don't have those data as well. Thank you.

>> Okay. I want to know about the process of blockage for Internet content and external content. Thanks.

>> Hi. I wanted some more clarity on how the three or four of you use the right information laws to get this kind of data. What were the things you were looking for in relation to the Internet and how did you go about it? What was the criteria?

>> EELING CHIU: Okay. So maybe who wants to answer a question? We have four questions. One is about gender, one is about the law about freedom of information, and you mentioned about the principle, Manila Principles. Comments?

>> BENJAMIN ZHOU: Hello. Let me respond to the access to information law question first because I think the issue in Hong Kong is a little bit -- I would not say terrible, but is not so good as other advanced economy because there is no system information law in Hong Kong so far. As I mentioned just now, we send the inquiry to

the government departments for court access to information. It's not a law. It was made in 1995 when Hong Kong was still in the British Colony under the governance of Chris Patten in response to some call from the democratic -- the democracy parties, which is the anti-China parties. So Hong Kong has such a code to handle the system information, but after that a lot of people, scholars, civil societies, calling for to make it into a real law, but Hong Kong Government continued to reject, including Hong Kong transparencies, according to make the access to information law. Because even though -- so let me introduce the situation in Hong Kong. It's access to information -- we can't allow us to send inquiries to the government and the government be responsible to respond. So far the Hong Kong Government did a good job, even the advantage citizens just send an email to any department to the officer in charge. They will respond.

But some departments, better than other departments. So that's why we have lack of a guidelines -- detailed guidelines about how an office is to handle such requests. But the most important thing is that we need to have the law to make it a mandate. Thank you.

>> Since China does not have a Transparency Report, I would like to only reply to the question of immediate library. There is a special clause in China's tort liability law which distinguishes two kinds of liability, which is trick liability and thought liability. Generally, it states that if ISPs is aware the user is using the Internet to examine information in violation of other people's -- sorry, other people's right, then the ISP has an obligation to notify relevant agencies and to take down the content in the first place. But it is quite controversial as to what amounts too aware of. That's the very delicate law between strict liability and -- liability. So so far I think ISPs are going to risk -- not to risk and just take down any information as well as they got notified by suspicious violations of law by those information. Yeah. Thank you.

>> Okay. For the first question about Manila Principles, first, it's a little embarrassing, but Taiwan in the past we seldom participate on the international principles. And it's some kind of related to our political programmes, but yeah. But I think it's -- I'm not sure because Manila Principle, it's about, the principle about content, right? Internet content? And oh, I don't -- don't have a very good answer. Sorry. But it's hard for in Taiwan to use international principle even though it is official one. And the Manila Principle is an official one, I think. Yes. So it's -- it has some difficulties here.

And for the second question about content which blocked, which type of content be blocked -- or mechanism. In Taiwan, last year we report we investigated mostly about -- we focused on -- we focused on iWIN, this organisation. And because iWIN will get our -- get our request from citizen civil society and so we put that effort in this area, in this organisation and tried to make clear what's the standard

transfer each case to different government. For example, which content you will be categorize as pornography or which content will be categorized as, I don't know, cyberbullying. Yeah. Such as that. But the fact, the fact is all we got is really, really limited. Yeah. iWIN, I don't know, iWIN, I really don't know why, never clearly talk about that. They have some statistics on their website talking about how many cases they receive and how many cases they have done -- means they already transferred to each government. But they don't talk too much about transfer, how they transfer. So yeah. Sorry. Not very -- but it's one of our men goes to try to achieve --

(speaker off mic).

>> Okay. Maybe I just --

>> Sorry, member of APNIC, basically I made a phone call to iWIN a few days ago because I need to prepare another section, that's what happened the day after tomorrow. Anyway, I tried to figure out what sort of process for the notice and take down. But eventually I just realize how they operate. Because I was not aware of this organisation. And they just told me they have a procedure and they have an industry practice how to handle that kind of request by anybody. Anybody can just request and say I need to take down some website and consider cyberbullied or pornography. So they will review the request and submit the request to relative government organisation or government authority or even requester that issued to the service provider. So several -- and technician after that.

My next question to him is how can you enforce that to happen? And they say if that obviously violated the rule. Are you a judge? How you can review that considered a violated law? They couldn't answer that question and event they tell me -- I tell them they hold a motto. We have 6,000 members, I think. So all behavior based on a best interest of our member. And what's a membership. And he says we have some member. And how can you say you have member, he couldn't mention how the member was selected. So just consider themselves as a modest to hold a motto, but they didn't realize how to perform a basic motto in practice about how to incubate a -- in practice. So that's what I know from iWIN point of view. So to answer your question, they don't have any legal basis, basically. They're performed a notice, but they don't -- they cannot enforce the takedown. They're just doing their best effort to take it down. And it is through their political muscle from different government agencies, that's what they did. And unfortunately, it's not very civilized.

>> Okay. Just to follow up. I forgot what I was going to say. The fact that iWIN -- last year tried to -- yeah. I think iWIN should publish list procedure on the website because they should do it, and even and last year we asked iWIN. And in fact, iWIN's responsibility is just for yes guys. They are founded or they are established by law which is related to the yes guys. So they are just responsible for the content which is not -- which is improper for yes guys. But

in fact they received all kind of content now, all kind of requests now. And they say we have to do that because citizen just send their request to us and we cannot refuse or reject the request. I mean, I tried to tell them -- of course, could reject request because it's not your responsibility to handle this cases. And if in Taiwan, we don't have any organisation or authority to handle these cases. That is the problem of our government. That is not a problem for you. So yeah. So that's just a follow-up. Yeah.

>> EELING CHIU: Does anyone want to add some conclusion? No? Okay. So do you have more question?

>> One.

>> EELING CHIU: Okay. Because we have to close soon. So yeah. Pretty short.

>> I mentioned the Manila Principles because I think they're quite relevant. They're about the reliability of intermediates for the content they carry. They set down the principles under which takedown orders should be given, the predict act and the reasonable sort of common law or natural law approach to these things. It's not an international treaty. It's a voluntary code which came out of the Manila rights meeting last year. It's available online in multiple languages on ManilaPrinciples.org they've been speaking to individuals and organisations to come on and give support to those principles. I do -- for anyone that's not aware of them, I do recommend having a look at the Manila Principle. It's a very good model for use of Internet users and technical organisations providing the services because it actually makes transparency the sort of number one sort of principle behind all of these intermediate issues. So I thought I would mention that in case it's not well-known. Thanks.

>> Just more information on that. There is a session on Manila Principles tomorrow. What time is it?

>> What time is it?

>> 4:00 p.m.

>> Which room?

>> I forgot the room.

>> Okay. We will join that. Okay. Thank you for the suggestion and the questions. I think it's a very good discussion, and we think maybe we should put more international principles -- I remember that EFF, they also have another guideline about the government surveillance online rights. So yeah. And also the gender perspective, I think, is also important when we request the information from the government. Maybe we should ask them to provide the statistics about the gender. Yeah. Okay. Thank you for everyone. And now it's time for lunch.

(Applause).

>> Lunch is on the second floor. Thank you.

(completed at 12:03 a.m. CST)

***

This text is being provided in a realtime format. Communication Access Realtime Translation (CART) or captioning are provided in order to facilitate communication accessibility and may not be a totally verbatim record of the proceedings.

***