FINISHED FILE

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

27 JULY 2016
ROOM 401
16:00
WORKSHOP 10
SECURITY AND MANAGEMENT OF
INTERNET CONTENT FROM OVERSEAS

Services Provided By:
Caption First, Inc.
P.O. Box 3066
Monument, CO 80132
1-877-825-5234
+001-719-482-9835
www.captionfirst.com

***

***

>> KATHERINE CHEN: Ladies and gentlemen, the Security and Management of Internet Content from Overseas will begin shortly. Turn off your cellphones and any sound-producing device. Thank you for your cooperation.

Before we start our first session we would like you to take a moment for group photos and moderators. Please all speakers and moderators go into the stage and take a photo. Our photographer Mr. Young will take a photo of you.

Thank you. Please take the stage.

Good evening, everyone. It is my privilege here to moderate this session for the Asia-Pacific Regional Internet Governance Forum. Thank you. The title of this workshop is Security and Management of Internet Content from Overseas. Why we're relevant to this topic? Consider the established Infrastructure trust of the Asia-Pacific region and the digital age converging, it is clear that the issue of Internet Governance is too important to ignore and challenges rise up to meet us, one of which can be clearly seen in the title of this workshop, Security and Management of Internet Content from Overseas.

We're fortunate to have five speakers who are experts in this

area here to share their viewpoints on this topic. We have planned three agendas, each lasting 20 minutes. After all speakers finish their presentations our discussion to each Agenda will continue. Each discussion will last 9 minutes with QA from the audience.

Firstly, I'm sure you agree that we're keen to get insight from some familiar companies and learn what steps they take when facing this issue. It is our great pleasure to be joined by representatives from LINE and from Facebook.

The first speaker is Mr. Takesh Nakayama. Takesh Nakayama is an executive officer at LINE Corporation in charge of security, legal affairs and the compliance. He's also the chief privacy and information security officer of the company. His talk is entitled Cybercrime Messager App.

The second speaker, Mr. David Caragliano from Facebook. Mr. David Caragliano takes the position of product policy manager in California. His team plans out global community standards to Facebook which looks at what content can or cannot be shared on the site. He'll share the topic Facebook Community Standards.

In the second subAgenda we'll focus on the opportunities and dilemmas every country encounters when looking at a fair, healthy Internet environment. It is a great privilege to be joined by Korean Communication Standard Commission and from Taiwan to share their viewpoints. The first speaker is Hyangsun Lee, who is a senior research Fellow of the Korea Communication Standards Commission. She worked as an associate editor for the Federal Communication Law Journal and senior researcher of the Korean Research Institute for Information Culture. Her talk is entitled enhancing cooperation systems for providers to better confront legal and harmful online content from overseas.

The second speaker is Dr. Bernard Kao, a board member who is known for founding a hotline, and he's looked at child protection efforts to battle sexual child exploitation and abuse content and human trafficking. He was also elected to the position of board member with our portfolio in '06. The topic that he'll deliver is entitled international efforts on combating online sexual exploitation of children.

Last but not least we will take this opportunity to share our views, NCC, with the public. Our Commissioner designate Jason Powell will give a presentation on Governance of Children Online Safety. He's been at the NCC since its establishment ten years ago and during this time he's served as the director of broadcasting content department and director of legal affairs department. He's deeply committed to respecting freedom of speech and he was responsible for establishing mechanism of coregulation in electronic media and the Internet regulation issues. I believe he's well qualified to illustrate the perspective of the commission concerning Internet Governance.

Now let's please welcome our first speaker, Mr. Takesh Nakayama.

>> TAKESH NAKAYAMA: For this brief session we'll talk about LINE and cybercrimes at LINE and solutions, we'll focus on three major issues of LINE and also touch upon security and safety of LINE and we'll wrap it up. Now, about LINE.

How many of you guys know LINE or use LINE? A great number. Thank you for using!

LINE, those that don't know, it is a global mobile platform for communication services. Our messager app LINE is the foundation over the platform, the app operation, all mobile operating systems with the app users communicate through free messaging instant messaging and voice and video calls.

Since the introduction of LINE messager in Japan in June, 2011, LINE has grown into a global platform with users in more than 230 countries, a very strong user base in Asia. Our active user base per month has grown to 218 million MAUs globally in March of 2016 with 152 million MAUs in four of the largest markets, which is Japan, Taiwan and Tai and Indonesia. In Japan we have 58 million users.

We provide users with a wide range of social and interactive content and services such as mobile games, music, payment services, job postings, restaurant reservation, taxi booking services and so on. LINE messager app serves as a smart portal to these applications and services. It is a large global user base which has big impacts on society. The magnitude of the exposure that's become a target of cybercrime.

There are various forms of cybercrime targeting LINE including identity theft, service exploration, social engineering, phishing attack, malware, ransomwear, unauthorized access. Among the crimes, today we're focusing on the crime in Japan, in particular we'll discuss three topics, account theft, LINE account theft, game cheat, spam.

Now game cheat, this typically involves an abuser trying to modify a game application in order to make the game easier and to get certain advantages. Even one of the typical adventure games for instance as a player your goal is, say, to save your Princess from the bad guys who capture her. You are ranked among friends and family based on the number of game points you win.

No question of how many of you play LINE games? No one? You? Thank you!

Now a special feature of a LINE game is that you can see your ranking among all your friends on your list. You see you're competing against your family and friends, and you can see how high up you are. You need to clear module stages to save the Princess and fight and defeat the bad guys before you can go to the next stages. As you clear several the stages the game becomes more and more difficult. To defeat enemies, you'll be rewarded with bonus points. With a required number of points, you can purchase certain items that will make your character strong, give your character some useful tools and ways to fight against the bad guys. In a typical game you need time and effort to make progress,

however nobody is so busy that you don't have the time. What do you do? Rather than spending time, you may buy time. How? By paying money to make character stronger, you buy extra ways, fighting against the bad guys so you can clear difficult stages and get lots of bonus points and do that without spending lots of time. To create the difficult stages, what would the abuser do? He may change the game illegally, just slow down the movement of the enemy to show that it is easier to defeat. Thereby clearing the required stages and getting lots of points with little difficult and little time. Very unfair. He may manipulate the game to get a large number of points in this way he could rank higher illegally and unfairly compared to other honest users. Further with the many points that he cheated to obtain cheating by some rare item and he can actually reach for the item for uses, for money. He will had also offer to play the game for some users for fee to perform the cheats on the account of the user. This is how the abuser illegally makes money. To prevent the cheats, LINE added a change detection platform. What it means, we have implanted a detection program within the game itself that alerts us when something out of the ordinary happens.

For example, it notifies when there is change in the bonus point perimeters where some users certainly get so many points within a very short period of time so that we have to look into that. Once we detected the cheat, we stop the abuser, freeze the account, look at the harm done, take back what was taken by the user and ban the abuser from the service. With the introduction of the cheat detection platform, LINE successfully reduced the cheat by 85% during the past three years. Despite this success, the abusers are always coming up with new tricks and newspaper ways to cheat so we are strive to be up to date on new technologies and improve our cheat technology program.

Let's go to account theft.

This is 85% reduction, account theft.

This is a major issue primarily in Japan. This can happen through an e-mail account and also a LINE account. The motivation behind account theft on SNS can range from simple prank to more serious attacks in that scamming or hurting someone's social networks, account theft.

The abuser don't normally use -- they use the following steps, three steps: Advise list of ID and passwords from legal websites.

Second step, then he tries to log in to the target SNS account by using the legally obtained information if he is successful he can highjack the account and have full control of the account.

He may proceed to contact the friends and families of the true account holder he fraudulently asked them for money or buy gift cards and they may actually give money to the abuser not knowing that the account has been hijacked. When the abuser gets money, he will go out and sometimes they'll log out and delete the account altogether.

In Japan, the scale of the account theft issue was so large in 2014 and '15 that it became a social problem. LINE introduced effective

measures against the account theft programs and for the past two years this included a PIN code identification set by the LINE users themselves in addition to their normal passwords. The authentication SMS, this is a factor of authentication required in addition to e-mail and password in case of account migration when users change their handsets we have block mechanism in the case of suspicious behavior. The measures just explained we're able to effectively authenticate our user identity through these efforts in Japan we have successfully reduced the number of account theft incidents to close to zero as the graph shows.

Next set. SPAM. We have the Wikipedia explanation here, the electronic spamming is the use of electronic messaging systems to send unsolicited messages, especially advertising as well as sending messages repeatedly on the same site. Advertisers generally use it because virtually there is no cost other than the cost of managing the mailing list. Spam is simply annoying but it can be more serious. It can be used to get complex information from users and induce user to websites to buy expensive services and goods or otherwise for other users. The spamming is similar to e-mail spam.

Other than using messages like the latest technology in machine learning and we have increased the precision in detecting the behavior of spammers that can circumvent the rules. We have been very successful in significantly reducing spam, spam, they'll continue to try to find new ways to get new users and we're always fighting the spammers with new technology.

This is the three major issues.

We move to security and theft. Yeah, our mission, the company mission, closing the distance. Closing the distance to bring people service information closer together that is we handle the issues concerning the communication and taking place with closer friends and family. That means that involve most important private information. This requires a highest level of security practice. Security strategy includes end-to-end encryption, true delete and the security certificate, the ISO27001 and we are the first to obtain both SOC2 and 3, they certify that our user information is protected against illegal access and they certify safety of not just the message itself but also that of corporation and management.

Lastly, safety protecting children's safety. To protect children's safety in Japan we provide the age verification system that -- what it is, users cannot search and find underage users IDs. We also provide over 1,000 schoolwork shops a day nationwide. We send our specialists nationwide to educate school kids, parents, teachers on the correct use of line and the Internet moral and legalcy.

To wrap up, I want to emphasize we at LINE take our responsibilities to protect our users very seriously. We know that in spite of our recent successes we can never guarantee that no abuses will occur. For that reason, we will continue our strongest efforts to protect our users in the more than Internet landscape.

Thank you.

>> KATHERINE CHEN: Okay. Thank you. Thank you.

Second speaker is David from Facebook.

>> DAVID CARAGLIANO: I thank you for being here today. Can everybody hear me all right? Awesome.

I want it thank you all for being here today.

(Speaking language other than English). Thank you.

As I said, I focus on our content policy. This is an area that we take really seriously.

Can I see a show of hands, who in the audience is -- has been on Facebook today?

Okay. Thank you.

Has anybody here ever had the bad experience of seeing something in their news feed that was disturbing or offensive? Thank you for letting me know. This is something -- this is something that I think of a lot. A lot about. This is exactly what my team focuses on. We're thinking about what sort of content do we allow on Facebook and what do we not allow.

What I'm going to do today, I'll talk about the team that makes those rules, my team, how we go about developing the rules, what you all can do would when you see something like that in your news feed.

First I want to take a step back and I want to talk about Facebook and talk about the scale at which we operate. It really informs how we think about policy. We're founded in 2004 and we're a relatively new company. Our mission is to give people the power to share and to make the world more open and connected. We provide tools in a platform. You create the content.

Every day billions of things are shared on Facebook. We recently passed a huge milestone for us. We have more than a billion people daily using our product. That translates to 1.65 billion people monthly. This is an -- this is a tremendous amount of content. We're talking about more than a billion photos daily uploaded to Facebook. 630 billion photos up loaded since 2005.

It is also worth noting that more than 84% of the people who use our platform are coming from outside of the United States and Canada. We really need to take a global approach when we think about our policies. Let's dive in to that. Let's talk about who makes these policies, how the policies are developed and why we need policies in the first place.

Who are we? Who is this team? This team that I'm a part of that makes these rules about what's allowed and what's not allowed on Facebook. We're a global team. We're in six offices around the world. We're in Europe, North America, and we're here in Asia. We have diverse backgrounds on my team. Some of us are coming from law enforcement, we were state prosecutors, others of us, we're Human Rights lawyers, worked for NGOs that were advocating for Human Rights, and, of course, there are members of my team that are from the Internet industry.

Actually I want to step back for a minute. Why do we need policies? Does anyone have any thoughts on this? On why we need policies? What Facebook, what any of these platforms would be like if there were no rules. What's most important to us? Does anyone have any thoughts?

Not irrelevant. Yes. I would say in order to retain customers people need to feel safe. That's the -- that's really the core of it all, right? If we want to make the world open, connected and make sure people share, people will not share if they don't feel safe. That comes first. It is also important to us to foster certainty and responsible behavior, and we want to promote free expression and sharing. In order for that to happen, people need to feel safe.

We have one set of policies for the world. They're called the community standards. It can be a challenge for a community as large, diverse as ours to have one set of standards. I'll give you a really straightforward example. This is an example of nudity.

When we go to places like Brazil or the Nordic countries in Europe, they actually tell us that our nudity policies are too restrictive. That's what they say. When we go to other parts of the world what we hear is our nudity policies are not restrictive enough and so my team is in the enviable place of needing to decide where we draw the line.

Our policies govern everything that we believe has the potential to endanger the safety of the people that use our platform. That could range from something like self-harm to hate speech to cyberbullying to graphic violence.

When we're thinking about these policies we just don't talk amongst ourselves out in California and say that sounds pretty good, let's do that. No. We talk to a number of key stakeholders both internally within Facebook but also externally around the world as we very methodically think through what the right approach is within Facebook we talk to legal experts; we talk to security experts. We talk to people like George here in the audience on our public policy team that's in Hong Kong leading off the greater China region to get greater insights in the markets of where we operate. That's absolutely critical.

Outside of Facebook we talk to academics. We look at empirical research. We're a tech company, we have a lot of data. We love to look at data and think about data. We talk to non-profits. We talk to law enforcement. We talk to government regulators, lawmakers and Human Rights activists.

Even after all these consultations have taken place when we're considering a policy it all comes back to three principles. First, is that policy principle? Is it fair? Are we providing the same treatment for everybody globally on our platform?

Second, is it operable? It is really important that our standards are objective. As I said, there are billions of photos, billions of pieces of content to share every day on Facebook. We have people that

are doing that content -- reviewing that content all over the world, doesn't matter where you are we need our people to make the same calculation in one part of the world as they would in the other and for that sort of thing to happen our standards need to be objective.

Finally, our policies, are they explicable? Can we explain them? Are they easily to understand? Most of the content on Facebook is good. Most people want to share what they had for dinner at the night market, a snack they had, that they had a new child, a new baby.

Some content has no place for our site because it is inherently harmful. We have an example of that.

Something that we have heard too much about lately, violent extremism. Certain violent organizations are not allowed to have a presence on Facebook. That means the organization can't have a page, and if you're a member of that organization you can't have an account on Facebook. It doesn't matter if you use that account for talking about the weather, talking about what's on TV, talking about what you had for dinner, doesn't matter. If you're a member of that organization, you cannot be a part of our community. No one can support, praise, promote these organizations or their acts on our platform. That's not allowed. If that post is reported, we will remove that and there is consequences for that person. Finally, you can't celebrate or promote terrorist acts, acts of violence.

I want to run through quickly the tools we have at your disposal for reporting content so that you can get some of this bad stuff off of our platform. Every piece of content on Facebook can be reported. Reporting is 100% confidential. Every piece of content, you'll see -- there is a little carrot -- let's see. See this. You have an option to say I don't want to see this, you can unfollow this person. Ultimately you're in control of what you're seeing and experience, what it is like on Facebook. You can click through, tell us exactly what it is you're seeing. This can help us give us some signals so that we can enforce on it. Make sure you click through, submit it so that we can review it.

I'm out of time so I'll wrap up quickly.

When you report content on Facebook we're reviewing it around the clock. We have teams based in six global offices around the world. We speak more than 40 languages. We're -- we're triaging this content that's reported to us and we're actioning the serious stuff first. This is something that we take really seriously.

And I'm looking forward to your questions, and it is great to be here.

Thank you.

>> KATHERINE CHEN: Thank you. Our first subAgenda is over.

Let's move to the second subAgenda, international, and the first speaker is Dr. Hyangsun Lee. Please.

>> HYANGSUN LEE: Thank you for inviting me to this forum. It is my honor to be here as speaker.

I'm Hyangsun Lee from Korea Communications Standards Commission, KCSC. I will start with a brief introduction of KCSC.

I have too much information in my presentation slides for only 10 minutes of presentation. Please excuse me for escaping, jumping the slides or speaking out of content.

KCSC was established in 2008 as an independent statutory agency which governs the content regulation of broadcasting program and Internet communications. These are nine categories of legal content which are prohibited by law, of circulation by law. KCSC regulates these contents. This is the flow chart of our online content review process.

I'll skip this.

If after our review, if certain content is decided as illegal then KCSC makes decisions on the work for correction which include removable of content or access blockage or suspension or cancellation of service use and labeling unwholesome content for use. Basically the recommendation for a correction by KCSC are recommendations which is not legally binding but certain cases. Rapid changes in the Internet communication has brought us some draw backs along with many benefits. Almost noticeably proliferation of the content that's circulated through Internet. As you can see from the table the proportion of illegal content out of total content for which KCSC issues correction requests has increased. In 2015 the proportion is almost 75%. In six out of top ten services in terms of the number of correction requests issued by KCSC are the service providers including Google, Twitter, Tumbler and thankfully Facebook and LINE are not included.

Total illegal content circulated by over sea service providers increased by 13 times between 2010 and 2014, mostly obscene content including sex trafficking information, content increased by 17 times. Regulating illegal content from overseas is very tricky. It is because there's a limitation with application of domestic law to service providers who have servers in foreign territories so KCSC makes correction requests to overseas content providers when we do that. It is difficult to notify the providers about decisions and to implement them.

Therefore, we have so far in general, we ask -- we have asked domestic Internet network operator such as telecommunication, Telecom companies to block access to illegal content from overseas instead of directly requesting that overseas Internet service providers which hosts the content will remove it.

There's also limitations with the accessible illegal content overseas from a domestic network operators, the access is less effective than removable of the delivered content from the source and it is -- it is not easy to bypass. You need to have circumvention techniques such as proxy services is, virtual private networks and others and access blockage is not possible for encrypted traffic for technical, legal, financial and other reasons. Currently 25 to 35 global Internet traffic

uses encrypted networks and by the end of 2016 30 to 50% of global Internet traffic is expected to use encrypted networks.

What is the realistic and effective solution? We don't know, but maybe we can think from a different perspective.

A significant portion of illegal content from overseas circulates through the websites of global service providers. Self-regulation by overseas service providers has some limitations. They do good job but sometimes they have limitations.

So we may need to encourage the global service providers to more actively enforce their self-regulatory measures and provides guidance on how they can better cooperate with domestic regulations.

This could be better off for service providers because they are increasingly facing more pressure from the market and users to come up with more effective solutions to legal or illegal content. Maybe one of the solutions is to encourage them to include within a cooperative legal cooperative system.

As one of the solutions we begin to operate core operative self-deliberation system, CSDS in 2012 and we begin, we started the system, the service providers are all domestic for major service providers but the system has expanded greatly and as of June, 2016 26 domestic operators had operated in this system and one of the most noticeable achievements is our influence off of the global service providers.

Facebook, Google, Twitter, and Instagram and others will join soon FC2 and I hope LINE will be.

Maybe I need to skip.

This is how the system works. We sort the items and we provide the information of the items and they review and take the counter actions and reply to us about the results. If there is no reply, no action taken, then the KCSC deliberation process starts.

Besides the potential solution I wanted to suggest a method that can, you know, encourage better cooperation among the service providers and national regulators, but because of the time constraints I'll finish my presentation here.

Thank you.

>> KATHERINE CHEN: Thank you.

Our second speaker is Dr. Bernard Kao.

>> BERNARD KAO: Good afternoon, ladies and gentlemen. My name is Bernard Kao. It is an honor to be here.

First of all, I would like to thank Katherine Chen, the Commissioner for calling us experts. Actually that reminds me of a rather satirical definition for the word expert which says an expert is someone who knows more and more about less and less until eventually he knows everything about nothing. I hope I'm not that kind of expert.

Now an English philosopher used to say it is impossible to speak in such a way that you cannot be misunderstood. To avoid more misunderstandings, I'm going to make my presentations very brief and

save the time for questions, comments, discussions.

The digital world is very wonderful and a colorful place to visit. It is not an exaggeration to say that we cannot live without it. For me I use LINE, Facebook, Internet Explorers, other things everybody day if not every hour so imagine how much important it is. Cyberspace is a very dangerous place, especially for children. A lot of bad things can be found on the Internet these are things we don't want to see on the Internet but they can be found easily though. I believe some of you have found this on the Internet, I have seen this. Among them, child sexual exploitation is most formidable. Now International Treaties, national laws have come to the conclusion that there are two types of online sexual exploitation of children, namely first child sexual abuse materials or child pornography and second, child grooming. They're often carried out by pedophiles, what are those? What are throws people? Well, a pedophilia is a psychiatric disorder where a man experiences sexual attraction to children. Oftentimes no pathological manifestations are found in these people. They look normal but they're dangerous. It is very difficult for government alone to fight against these activities since the Internet is transnational and anonymous and interactive. An online safety network is necessary. What do we do?

Let us take a brief review since the Rights of Child came in effect in 1990. The international efforts we see the 1996, the World Congress against the commercial sexual exploitation of children, they were able to reach some conclusions about how to deal with these issues and then in 1998 the Interpol, international police organizations, they held an expert meeting and in the 1999 UNESCO meeting, sexual abuse of children, child pornography and pedophilia on the Internet. 2001, Second World Congress and then we have some international organizations established, namely Inhope and Insafe and then were the 2004 cybercrime conventions a comprehensive treaty doing with all kinds of illegal activities on the Internet, including online sexual exploitation of children. 2005, the VGT, the Virtual Global Taskforce and the next year, want Financial Coalition Against Child Pornography. 2008, World Congress against sexual exploitation of children and adolescents. Followed by 2009 Interpol, another General Assembly to tackle the issues. I have seen a lot of international efforts trying to deal with these things. In some, we reach a conclusion that it is a triple alliance of legislation enforcement, industry and NGOs.

For the legislation and enforcement both substantive and procedural rules which can cope with new technologies are needed. To date, it has been agreed that the law should punish producing, selling, disseminating and possessing child sexual abuse materials and grooming for the purpose of sexual contact. Now I'm not going to go into details about this legal comparisons because as law professor I can tell you it is extremely boring, I'm not going to bore you.

I'll just skip it. I believe you all agree.

For the NGOs, the NGOs can do a lot of things, establishing hotlines, help lines, ratings, education, also international liaison. I would like to emphasize about the work of international liaison because to deal with this illegal activities on the Internet, if we have to do it by government to government, communications with government to government, then it is a very time consuming thing because there are a lot of procedures to follow. We need to do it swiftly. NGO should take the place of doing this international liaisons. We don't have this bureaucratic practices, procedures so we can do it faster. The NGOs can have connections with NGOs of other countries, for instance, Taiwan, which I'm a board member, we have contacts with 60, 70NGOs all over the world and we can also have contact with international NGOs Inhope, Insafe in particular and then we have connections with Interpol and the Europol so we obtain useful and exchange useful information.

The industry can do a lot of things. Donations, please give more money, you can do a lot of things, you have the big money and self-regulation, you develop self-regulatory rules. Policies turning into legal rules. Also developing new techniques, filtering techniques, tracing techniques, photo DNA, et cetera, we use new technologies to deal with the new criminal activities on the Internet and also the financial collisions. We tried to have visa, MasterCard, Yahoo, others more famous, more Internet, the companies to cooperate together so that those illegal activities when they're doing this illegal sort of money exchanges we can cut them off.

Here comes a question: With this triple alliance do you think that we can eliminate child pornography and child grooming once and for all? The answer is no. Objective the contrary, if we take a look at the recent statistics published by some international organizations we can see that the situation is actually getting worse. We just have to keep fighting. In 1982 it the United States Supreme Court New York versus Ferber gave us a line that the democratic society rests for its continuance upon the healthy well-rounded growth young people into full maturity as citizens. What does that tell us? The judges are trying to say that child protection, it is not just about protecting children, it is also about preserving and improving our democracy.

Thank you. That's all.

>> KATHERINE CHEN: Okay. Thank you. Thank you.

Our last presenter, speaker is Dr. Jason Ho whose perspective is on Taiwan's perspective.

>> JASON HO: Good morning, everyone. I'm Jason Ho from National Communications Commission.

In Taiwan we're concerned about the Internet Governance. Our practice on Internet Governance is in line with this forum.

I'm going to entrust our -- I'll go to my common tongue.

(Speaking language other than English).

What he said, regarding it child pornography, cybercrime, but what I'll share with you today, it is why we care about for parents, about the daily lives, about exposure of murdered children on the Internet.

In Taiwan in 2003 the government has commissioned a government information office to classify the Internet. We started the Protection of Children and Youth Welfare Act in software screening all the way to PICS and TICRF. This is the first case in Taipei where the city government accused the NEXT media for a fine of more than $1 million.

To the control commission the executive to coordinate the technology center where the security team, they have a set of the so-called cyber safety mechanism.

In 2012 we have amended the paragraph 1 of Article 27 of the protection of Children and Youths Welfare and Rights Act and in 2014THIH was dismissed.

In 2013 the single window highway established that Institute of Watch Internet Network where the NCC collaborated with the Ministry of Education, Ministry of Culture affairs, health and welfare and the interior Minister of interior and economic affairs.

There's seven major reals for IWIN such as to observe, study the IP behavior on the web or receive the complaint from the general public, et cetera. IWIN started from an Internet classification, rating to a single window service. This is a kind of pattern from the bottom to top mechanism where they'll report the violation to the government agency. Prior tore 2013 we have received around 5,000 reports this year, the 2014 since our incident, the case jumped to 15,000. The majority of the cases are Internet pornography related however some of them are just indecent.

I would like to take this opportunity to express our government's appreciation to the ICP or IPP provider where they have 67.82% of take down, however we're happy to have five cases with about a million dollars' fund. Our goal is to find patterns between the freedom of speech and children protection. At the moment we have three challenges, the last years complained we have more than 5,000 complaints where more than 50% of them came from overseas. At the moment our major challenges are the limited ability to investigate the website contents overseas.

Second, technology advancement, in 2040 we have over 18,000 criminal cases committed online, with that, I'm happy to see a branch office here inner Taiwan.

We talked about the encryption on mobile devices that's made us more difficult and our challenge is the access to overseas Internet platforms. for the past few years' ache see that the Internet, this is not feasible.

With regard to notice and take down, the issues are who to notice and does it is carry the judicial authority and who is responsible for that.

As do international cooperation, as mentioned that Dr. Kao mentioned we should set up a hotline or sign a regional agreement, we would rely on the technology to solve it, it for example the parental control or the photo DNA. This year we have proposed an electronic communication act Articles 18 to 20 in line with the Manila principles. Currently we're the applying principles of intent policymaking such as partner up and coalition with private sectors.

I would like to once again emphasize the equal importance of protecting children's safety and also the right for Internet propaganda.

Thank you very much.

>> KATHERINE CHEN: Thank you. Thank you.

We have a few minutes left. According to the staff, we have equal time slots for each Agenda. 3 minutes for Facebook, 3 minutes for international and 3 minutes for Jason.

Any questions for the floor?

>> First question is directed to Facebook.

Identify your name and your affiliation.

>> I'm Ka. I'm from Human Rights NGO in Malaysia. This question is for David from Facebook.

I'm a woman. I would like to know how Facebook justifies that a picture of me breastfeeding is a threat to your server security? How do you justify that information about women sexual health is a threaten to user safety?

>> DAVID CARAGLIANO: Thank you for the question. It is important to note -- let me ask, did you have an experience where that content was removed from Facebook?

I would like to -- let's circle up. I want to learn more about those examples.

What I can say as far as the global community standards go is that we allow breastfeeding on Facebook. That's an exception to our nudity policy. We allow those images. I don't know this exact example. You know, it's possible -- there are a couple of possibilities.

One possibility is that we make mistakes. That when you operate at a scale in the billions that means that we get millions of reports every week. It is possible that someone reported that image and one of our viewers made an error and took it down. When that happens, it comes to our attention, we try to move fast, we try to apologize and restore that content. I want to learn more about that example.

I'm not sure this is the case in Malaysia. There are isolated, rare circumstances where our standards are not in line with local law. It when a government makes a valid legal request that a certain piece of content violates local law, we do -- we can remove that piece of content. That does happen. We're transparent about that. We report that in our transparency report for everyone to see in the world. I don't know exactly the circumstances and I want to learn more about it. Let's talk afterward.

Thank you for that question.

>> KATHERINE CHEN: Next question goes to --

>> (No microphone).

>> Sorry, tell me where -- your name, where you're coming from

>> Pakistan.

>> Excellent.

Hate speech.

>> (No microphone). -- it is basically hate speech about some religion minority particular group. I reported the case to Facebook but my request was turned down. I was just trying to ask how do you make sure that such posts, how do -- they do not meet your community standards because it was clearly a hate speech. Then there are similar -- there arer a number of organizations banned in Pakistan and they're operating with different names, running Facebook pages and one from Pakistan can easily identify it because they do not use their names, they use particular certain pictorial images like the flags, slogans, stuff like that, anyone from Pakistan knows this is a banned organization running a page with a different name. How do you make sure that these organizations are not running the pages with a different name?

>> DAVID CARAGLIANO: Those are awesome questions.

Let me unpack that. There are two issues I'm hearing. One relates to dangerous organizations that had a presence on the platform. The other, related to hate speech.

First let me say, hate speech is a really nuanced policy, a really hard policy. I think it is important that we have it because it's important for us to say that certain sorts of attacks or dehumanizing language against groups of people that have protected characteristics like religion, ethnicity, they're protected. That's important to take that position. That being said, it can -- there are line drawing problems. Let's come back, talk about that specific example and we'll evaluate if that's an error on our part which I said happens. Or whether maybe that's one of those edge cases that doesn't sign -- violate communities standards.

With respect to dangerous organizations: You reported it. Okay. I -- I -- so what I can say is that our reviewers are -- it was reviewed by -- that post was reviewed and they need to be able to tell from the context that that is actually one of those banned organizations. Now there may be other ways for you to escalate content like that if it is not working by reporting it in product. That's something we can touch on.

Thanks.

>> KATHERINE CHEN: Yes.

>> Thank you. I'm Andrew from the Regulatory Telecom Service.

My question to David, I would like to know if Facebook sort of has some relation with governments in some ways specifically or does that fall into individual -- on an individual basis? I'm asking this

question because we have -- the population, it is about 280,000. We have a group that is about 30,000, a Facebook group, a lot of discussions leads to discussions on anything, it is just opened. Some languages and things used, abusive and also a lot of confidential data has been posted online.

The government is wanting to communicate with the Facebook but they do not know how. Maybe we'll talk later. I want to know if there is a communication channel there for governments and we had just an example. Our prime minister, the speaker, they be don't use the Internet or the Facebook but somehow in that group someone created a profile in their names so thank you.

>> DAVID CARAGLIANO: Sure.

Our regional -- we have a regional public policy leads around the world. I think that the best thing is to put you in touch with that person. They're in touch with me, my team, on a regular basis.

What I'm hearing from you, there are a number of things you touched on that relate to human standards and impersonation. It is one of those things, nasty language maybe, sometimes it violates, sometimes it doesn't -- on a platform of our size people are going to say offensive things sometimes and we want to allow people to express the full range of emotion.

You mentioned private PI, that's something that's not allowed on Facebook. You can't share someone's private information and there are ways to remove that as well.

As you know, we have a real name policy, a fake profile like that ought to violate -- did you report any of this content? Do you know if any colleagues reported any of this content?

>> Not corporately, but I don't know individually as well. We're not really sure about the reporting system, whether action will be taken or if the report is anonymous or --

>> DAVID CARAGLIANO: Yeah. All reporting is anonymous. Oftentimes the quickest way to get violating content off the platform is to report that content in product.

Every piece of content on Facebook, doesn't matter if it is media, an image, a video, a live video, text, all of that can be reported. We should action that sometimes within a couple of hours.

Every time that you report a piece of content you will receive a message in what we call the support inbox and you will get a red jewel notification saying thank you for reporting that content. When we make a decision as to whether or not that violates you will get a response.

We try to be transparent and communicate with our community because we really rely upon you all to identify violating content. We like to think of our system as the world's largest neighborhood watch organization, we really depend on you all in many ways to identify and report violating content.

>> Thank you.

>> I'm from Taiwan.

I used to manage copyright issues. I used to run a little Facebook group that we would discuss about games. There is often people coming in posting pirated copies and when we tried to report it, Facebook just told me if I want to report copyright content I need to be the copyright holder. However, that's not even possible, we're not like those big-end companies. We could just only delete it, those posts one by one in our group. Is there any way that can be resolved? If there are publicly available paid content, we can report it without actually being the copyright holder.

>> DAVID CARAGLIANO: So I think it is a great question. There are -- there is another team that's really expert on copyright issues. It is actually not my team.

To my knowledge, I think that's right. I think you have to be the copyright holder to report that stuff.

Can I ask, was this a secret group, a closed group, an open group

>> It was an open group. This also happened for non-open groups.

>> DAVID CARAGLIANO: Sure. Sure. Sure.

I mean, if it was an open group I think that's fair game. I think we have -- we may have technologies in place that the IP team could speak to closely that would detect this sort of stuff, certainly in open groups. I think you did the right thing by deleting those individual pieces of content.

>> Thank you.

>> I'm from Burkina Faso and I'm studying here.

I grew up in France. I have been in France 12 years. I have seen during the terrorists attack in Paris, I have seen that Facebook has some notification just about security, like telling me that my friends are safe and everything. I have noticed that every time -- there is a terrorist attack in countries like France, U.S.A., Facebook just gives me a notification. I also noticed that when there is some terrorist attack in Africa, for example, in my birth country, in Burkina Faso, during the French attack we had an attack in my birth country but Facebook didn't notice anything, didn't say anything. The security content of Facebook, is it a right or a privilege?

>> DAVID CARAGLIANO: A great question. Thank you for asking.

What you're talking about is a feature called safety check. Again, this isn't something I work on directly. I do want to say within the company this issue that you've raised of where we operate safety check and when is something we're thinking a lot about. I think we also put a lot of emphasis on something called unconscious biases. It is something that effects all of us. We want it as a global platform, we want to make sure that's not effecting how we use safety check.

This kind of feedback that you're giving, it is really valuable, it is really important. It is actually something that, you know, we're thinking about.

I think in general safety check is a new, a relatively new feature, we're still working out exactly the standards around when we would activate it. This is super valuable feedback and I appreciate it.

Thank you.

>> KATHERINE CHEN: As a moderator, I have to say that the time is really running out. We're sorry. I have to conclude the session. I thank you, all of the presenters, and audience for the great questions.

Thank you.

***

***