FINISHED FILE

ASIA PACIFIC REGIONAL INTERNET GOVERNANCE FORUM
EVOLUTION OF INTERNET GOVERNANCE:
EMPOWERING SUSTAINABLE DEVELOPMENT
MACAO 2015
2 JULY 2015
N HALL
11:00 LOCAL TIME
SURVEILLANCE TRENDS, CHALLENGES AND OPPORTUNITIES
IN ASIA PACIFIC
CRITICAL INTERNET RESOURCES
SESSION 38

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

***

***

Live captioning at APrIGF Macao 2015 is brought to you by Internet Society

>> Welcome, ladies and gentlemen, to our workshop on Surveillance Challenges, Trends and Opportunities and Possibilities. Thank you very much for your time.

I work for Bytes for All Pakistan. This workshop is organized with the Citizen Lab and we have panelists from all over the region. I will request our panelists to please join us on the stage, a professor from Citizen Lab, and Donny Budhi Utoyo from ICT Watch, Indonesia and Irene Poetranto, please.

Apologies again for starting late. We had only 5 minutes before the previous panel to do setup.

It was 2013 when we finally started getting some evidence of targeted surveillance and some revelations that this is happening in our region. It was thanks to Citizen Lab research that brought attention on what tools were being used by the governments in terms of surveillance and in different countries.

When we updated the report, we learned there are many more earlier reports in Pakistan, others, we began to know that there were many more Asian countries that were also using, for example, other regional surveillance tools and softwares for surveillance. Then we came to learn about the agreements between the different countries, Pakistan, Singapore, other countries, we want to understand this whole dynamic today and precisely for that reason we have our panelists over here. I'll first request Irene from Citizen Lab to give us an overview about the situation in the region. She'll talk about the research aspect and the current updates and findings. After that, we'll go towards our other panelists to get some country updates as well. Then we'll open the floor for question, answer and then discussions. Since it is birds of a feather reference, all of you can be engaged in this panel and I'll give you the floor. Thank you very much again.

Irene.

>> IRENE POETRANTO: Thank you, Shahzad. Thank you for the introduction.

I'm Irene Poetranto. I work with the Citizen Lab. I wanted to get the sound to work. It didn't, so we'll watch the video without sound.

This is a commercial made by Hacking Team, one of the companies that make surveillance systems. It is just a short video that we'll play right now.

He looks really friendly. Okay. If you want to watch the video with sound, that's the link. Okay. So just a quick introduction, like I said, I work for the Citizen Lab, we are based in the University of Toronto, Toronto, Canada, we analyze cybersecurity issues from a Civil Society perspective. Just briefly to summarize the work we do, we do research on three themes, targeted digital threats against Civil Society groups, surveillance and we do technical measurements of information controls and threats to freedom of expression and filtering and we have done work on information controls and corporate transparency, looking for use of data by telecommunication companies. We use the word information controls a lot and define it by actions constructed in or through information and communications technologies which seek to deny, disrupt, shape, secure or monitor information for political ends. We're interested in the digital arms market, it is a growing industry. It is current estimated to be worth at least $5 billion. A lot of the products and services, they're made in the west such as the United States, United Kingdom and sold throughout the world with few restrictions. Through our research we have found that some of these products ended up in the hands of governments with poor human right track reports, including the Bahrain, UAE and

Vietnam. This is an example of an event where government and law enforcement agencies can purchase these tools and equipment.

First of all, I'll quickly go through to a tool FinFisher which is a line of software developed by Gamma International and it is sold exclusively to law enforcement and intelligence agencies by Gamma based in the U.K. They have a lot of tools, one capable of intercepting e-mails, instant messaging, and spying on users through web cams and others. This is a sample of the feature they ties, an easy to use interface, bi-passing antivirus systems, full Skype monitoring, live surveillance, key logging, so on, so forth.

This is an example of a fin spy at work targeting a Human Rights activist in Bahrain and it is Melissa Chan's e-mail, she actually exists and works for Al Jazeera. This is quickly some of our findings. We fingerprinted the FinSpy unique fingerprints and we have found them in 36 countries in the world, some governed by authoritarian regimes, Bahrain, Bangladesh, Brunei, Ethiopia, this has been used to target Human Rights activists and opposition political groups in Ethiopia and Malaysia and the link is right there if you want to take a look. This is a *New York Times* coverage of our report when we found that the software is being used to spy on dissidents. Quickly on our findings in Bahrain, we received several pieces of malware obtained by Vernon Silver, he's with Bloomberg news which were sent to a Bahraini prodemocracy activist, and we do this work to understand the malware and the actors he behind the attacks and risk to victims and we have several approaches, we infected an official machine and monitored the file system and the networking running information and it suggests the use of FinSpy which is part of the FinFisher intrusion kit.

This is an article, if you would like to read more about FinFisher in Bahrain.

This is a map we published which documents the presence of FinFisher around the world, we found it in 36 countries around the world. It is part of our report called "For Their Eyes Only, The Commercialization of Digital Spying." This image is from a forthcoming report which I can't talk about because we'll publish it at the end of the month. It shows Indonesia and lines converging. These are FinFisher servers and proxies located in Europe, Asia, et cetera, just to show how widely spread the network is.

The impact of our research, following the discovery of FinFisher servers on two Mexican ISPs, there was a lobbying for the Mexican government to conduct an investigation into how this is deployed in the country. We'll have an update on that.

The video I showed earlier, it was on Hacking Team. Hacking Team, it is another company that provides a commercial intrusion and it is a Milan-based company. They manufacture a product called Remote Control System, which is a Trojan sold exclusively to intelligence and law enforcement agencies worldwide. They describe as the video showed, she described the product as the solution to monitor targets using encryption or located outside of the borders of the government that wants to monitor them. This is an example of how they advertise their product.

This is from a brochure that they published in 2011.

So how does Remote Control System work? They infect a computer or mobile phone to intercept the data before encryption for transmission and can get data which was not encrypted, it can turn on a device's web cam, microphone, it can spy on the user and look at other information.

So we found Hacking Team has been used to target a journalism group in Morocco, they monitor a website which is critical of their government and we found evidence that the same surveillance was used to target a Human Rights activist based in the UE. that served 7 months in prison for signing a prodemocracy petition. We have identified countries around the world that we suspect are users of the Remote Control System and we found that the computers that are infected sent the surveillance data back through a series of servers and in a circuit chain to prevent someone discovering the spyware or infected computer, they can't trace it back to the government. This is a map that we produced mapping the presence of Hacking Team worldwide in Asia their president, Thailand, Korea others. Just a bit more on the findings of Hacking Team, we have a series of reports, we analyzed these chains and found U.S. based dedicated servers are part of the Infrastructure implemented by governments, we have also reported -- the report made the front page of the Washington post that U.S. journalists were targeted on U.S. soil by the government of Ethiopia and we have identified cases where the spyware servers were disguised as websites of U.S. companies.

Again, that's a -- that's a brief overview of the work we do on commercialization of surveillance if you would like to read more on FinFisher that's the web address and on Hacking Team and I'm here to answer any questions.

>> [Applause].

>> As Irene in her presentation mentioned about Pakistan, quickly I'll give you a bit of an update on what's happening around that case and other developments. In 2013 when we came to know about Finfisher we went to the high court on this issue, we filed a petition. At that time it was already established that Pakistan is one of the -- we have a large citizen database, the largest in the world and we realized other trends of how

surveillance is happening. There is several different types of it. So we have come to know how, for example, the U.K. government, other governments, they're also spying in Pakistan and then we moved the investigation to the U.K. as well and it is a very important case now, it is --

>> (Please stand by for technical difficulties to be corrected).

>> Unless you don't have evidence, you can't fight the battle in the code or in the Human Rights movement as well. So in this situation we have seen that the digital surveillance has not helped anything in the security situation or in fighting terrorism but it has caused a lot of other problems as you can see with the whole chaos and the problems, the modern terror as well in the country.

There are two important updates to follow and we'll keep you all updated, one is a case in the Pakistani code and the other is in the U.K. investigative panel, the tribunal in the U.K. against GHQ. That's the update from Pakistan.

I now would request Professor Ang to give us an update on Singapore.

>> PEN HWA ANG: I'm going to go through the slides. All right. Sorry about this.

An update on the surveillance in Singapore: Singapore is part of this group. This -- I'll show you the bottom. The U.S., U.K., Canada, Australia, New Zealand, Singapore contributes intelligence to this group.

I think it is no secret that we spy on them, they spy on us. It is only fair. It is not a secret or in an expose, we just know it. I think the news, with the information to the U.S., but you see that it is in the context of the fears of the terrorists groups and most recently this.

You see the network here, I don't know if you know, but this is very, very sophisticated. There is a report that the U.S. was able to detect the Russian Telecoms cable and the Russians thought they were uncapable to, they sent a transport device and others to go down, they never expected someone would tap.

This is the cables and I don't have the report, I was looking, a report says that one condition for the cable to the U.S., a condition, the cable has to be open to access by intelligence agencies. It is not just that it is here, the mechanics here, in the design, you have to allow the intelligence agencies to access.

Inspiration for such surveillance comes from -- this is 2002, now ten years ago, it is from sending power, so the report, it says develop M16 rifle, stealth technology and Internet and it talks about military hardware -- he didn't talk about the military use but about the use of the intelligence information, you see in the bottom, the last two lines, the enormous amount of electronic information and analyze it for patterns of suspicious activity, mainly potential terrorist attacks. In Singapore we're focused on identifying the bad guys. I myself I propose projects looking at increasing security as an ecosystem. For example, in Australia I read that the police -- this was in the past -- they go around F they see a wi-fi open, they tap on the door, they say that the wi-fi is open. That's a way of increasing security of the whole ecosystem. When I say hey, how about a program like this, that's a good idea, the people were looking at this issue of intelligence and security, they were totally not interested. You could see their eyeballs rolling up, yeah. They were very interested in identifying individuals. So Singapore, the report is to identify individuals against terrorist attacks.

If you read, this is an article that's available on foreign policy. The issue is July of 2014, Peter Ho, he's now retired as the secretary of defense. The interesting thing on this quote, it is -- well, in the article Ho, he said that he was sort of surprised what users are doing with all of this information, the tracking, sort of the guts, that they had the gall to do this stuff. He was surprised and sort of inspired to do the same thing with Singapore.

In Singapore, we adapt things as usual. In Singapore we're testing how the surveillance may prevent terrorism and also the question is can this technology build a more harmonious society? I see some are smiling. The Chinese, you know, they -- they play on words, the harmonious society, it is sort of a play on words around that. This is a question that Singapore is asking, can you use this technology not just for terrorism but to improve social harmony.

This is my last slide because we're in a short amount of time. This is the last slide.

Having said that, this is ten years ago now, and there were concerns about surveillance, but it died down when the terrorist attacks happened, and now because a lot of the issue of surveillance and the revolution of Edward Snowden, there is some concerns now of the surveillance, this is a piece written by the dean of the law School of Singapore. He begins by saying this, it is interesting how he begins, you can reflect on the tone of the article, how should we balance liberty and security? The answer is simple, we shouldn't. We shouldn't have to balance liberty and security, we should try to do both.

An interesting thing is this, Singapore is very complex for some much this stuff, Simon, he's a white guy from England I believe, he's not an Asian, you know, it seems like Asians, we're less concerned about surveillance, why are these white guys talking about it? It seems okay. The dean of the law school, he married the daughter of the president of Singapore who was a politician, who was also a defense minister who had put in place some of the surveillance we're talking about. I say that he has an interesting family reunion discussions. There are many issues.

I want to end to say that I have -- I look at even myself, wonder why we have less concern about surveillance. We have little -- I know for example that I have -- with Internet security, you know, we joke, you know, that, hey, you have to be somebody to be done surveillance to, you know, it is more like a badge of honor but it is a strange thing. We thought that surveillance is done, we don't seem to be that concerned. Maybe that's something up for discussion. I want to end on a note, there is pushback, it is not -- it is not supported all the way, there is some pushback from some groups.

Thank you.

>> [Applause].

>> SHAHZAD AHMAD: A few years ago privacy, for example, in Asia was also a Western concept. People would say no one is concerned about that. Now the trend that we're seeing is that a lot of governments in Asia, they are introducing new legislation and the number much times policy laundering is happening from other countries to legalize, you know, all the different, you know, aspects of surveillance, filtering, and other technology. The problem is, in the developed world, there would be some protections available to the citizens. There would be privacy Commissioners, there would be information security Commissioners where you can -- where if there is a problem you can go and get some remedy or redress. In our countries, this is not happening.

We also need to aggregate for some basic protections when such policies come onboard in the countries.

There is a lot of noise now in our parliament as well. There has been discoveries of how premier intelligence agencies of the country are surveilling or spying on those in parliament and then thousands of people -- there is a list of 25,000 people which was submitted to the Supreme Court in another case that this is what they're doing in Pakistan. Still, we do not have ample information, there is much more to come. It will continue to come. We hope it will be -- you know, Snowden, he would bring us more information, our research lab like Citizen Lab would have mother evidence on this. I would now request Donny, he's from ICT watch from Indonesia, please update us.

>> DONNY BUDHI UTOYO: Still waiting.

>> SHAHZAD AHMAD: You need technical support? You opened

it already?

>> DONNY BUDHI UTOYO: No. No. I can't open the PowerPoint for some reason. Let's see.

>> SHAHZAD AHMAD: Can you start without the slides and then the slides will come?

>> DONNY BUDHI UTOYO: There is something happening that I wanted to share.

>> SHAHZAD AHMAD: Can you --

>> DONNY BUDHI UTOYO: I would rather use the PowerPoint. All the data is the actually in the graphic, it is -- I try to open it up first.

>> SHAHZAD AHMAD: Can you come, please?

In the meantime, he can figure out the --

>> DONNY BUDHI UTOYO: Will this one open?

>> Maybe you can try to export it.

>> DONNY BUDHI UTOYO: Okay.

>> ARTHIT SURIYAWONGKUL: Quickly -- sorry. I should be here. Right. I will quickly, I will talk, these actually happened in a year so far, that demonstrate the packages of surveillance in our country. I would just like to mention about what was talked about, I think it is more and more a tendency in this region to maybe accept surveillance as a kind of -- not really surveillance but just as a monitoring, the data collection, as probably more of a norm and one of the -- one of the -- there is better performance now in doing things like providing better public services is coming as well. In Singapore, people are more and more discussing about a smart nation, when you install all of the sensors, what it would be. I think actually tomorrow we'll have a session on that, the secrecy and privacy. I think more and more there is thoughts of the government or others, they'll collect more and more data in order to provide better services, it is coming stronger and stronger as well. I think that's the direction that we could probably -- that we'll now have to be more prepared for and actually think more about that.

I will come back to my country.

Since last year we found out -- actually this is probably not that so sophisticated as the FinFisher but it is a thing actually like -- it is very basic, it could affect a lot of people, it is actually working on the platform that I think it is one of the most popular in the country so there is two social networks, the first one, it is line, probably now they have about 33 million users in Thailand and the second, it is Facebook which has around 28 million users. I'm talking about Facebook first.

This is a page when you are in Thailand and you try to access websites, it probably has content that the government feels like is not so good for you to read or to watch, your ISP will redirect you to this page. It basically says I'm sorry, sorry for your inconvenience, the access to this data has been suspended by the authorities and the ministry of information and communication technology. If you would like to ask more about this information, you can contact -- there is a list of addresses there that you can contact.

Anyway, as you can see, there's one small button at the top-right corner, you see that button, right? Yeah. That blue one at the top. Once you click on that, what you actually expect when you go to hit that button, the window should be closed, right, and you continue to surf and you say, okay, I cannot access this website, you may be close it or go to a different link, but the thing is, when you hit on this close button, it will show you this Facebook app, is Locking, the window on the left. It will show you your Facebook page, and then there will be a dialogue box asking you would you like to continue to allow this app to collect your user name and e-mail or not. Most of the time when users see this they think, okay, probably, they -- I closed the landing page. This page, it is already gone because I closed it. Maybe going back, turning back to my old Facebook, because the app name, it is quite confusing so the name of the app is called locked in. So people think I'm going to go back to my face become and they hit okay. When they hit okay, it is like, okay, we'll collect this, whatever, and most of the time people are just like okay, let's just click it. This is not a thing that actually -- it is not that sophisticated and actually to be fair, every Facebook app collects your personal data anywhere, right, it is just how much they're able to collect that and extend. Some of the apps, you use the names and some of the apps, you're asked to give them the contact lists and whatever else the permissions are. This is kind of a normal thing for Facebook apps to do, what's not normal is actually this app tries to confuse people and when you combine this together, with the collecting personal data and knowingly from which you have -- people try to look where you were before you land on this page. You combine the two things, you say, okay, Shahzad is trying to access this website that's blocked in Thailand, you link it altogether and, you say, okay, in trying to do this, what kind of information is he trying to access which is not allowed? This is one of the practices that have happened around July, last year, and report this and after I think half a day after we read about this, they removed that button, but the app was still going on for around two more days before Facebook took this app down.

I think this is not the thing that really is applying here but mainly things about the -- maybe more or less the same things that happen during the occupation in Hong Kong last year, there was a fake app and basically -- people were downloading the apps, okay, the system will ask you what permission you will give to the app to collect the data. This app, it does the same, it asks permission to collect data because the protesters think that this is a legitimate app but actually the publisher of the app is not related to anything to the organizers of the occupy movement. They tried to confuse people that this is a legitimate app and collecting data. That's one thing.

The second one I want to show you about, the app names of the government trying to monitor the private communication of the users. The government claimed last year that they can -- this is a quote, we can monitor nearly 40 million live messages sent by people in Thailand each day. We don't know if this is a real claim or if technically they can do it or not. After this they actually rely on a carrier in Japan, they own the lines, they say technically it is impossible for anyone to actually do this because all the messages sent by this app, it is encrypted. We don't know if this is a good claim or not by the government. It actually shows that even in the private communications, if you want to do that, they can access that even with something like that.

Talking about encryption, we turn to this third example. This is a letter from the ministry of ICT, December, last year, so basically it is talking about setting up of the Committee to -- it is a working group to test the equipment to decrypt communications. In the letter it says because in the past the national policy for peace and order. It is basically the coordinator that took over the government last year, they issued an order to ask the ministry of ICT to monitor the content online and also to filter the contents.

In the letter it says because of this encrypted communication it has made the work of the regional ICT more difficult so in order to make the filtering, the monitoring work and go more smoothly it is necessary to setting up another working group to test equipment of how to decrypt this encrypted communication.

In the letter you see, the only probably English word there, it is SSL I think. There is another word there, international Internet gateway. The letter said it -- the first thing, okay, the test equipment, the second thing that they want to do is collaborate in the technical area where the ISP and also the operators of international gateway on how this equipment will work with those systems. I think this is an interesting move. In the same week the local newspaper published news that there are several local IPs reporting that there are officers from the ministry of ICT contacting them to test equipment. I think this is actually really happening, going on, it seems like six months ago, already, this is already July, so we not only show what will happen at the moment, this is the latest document that we have seen. After this, we cannot really get to our source. Anyway, we think that the technique they'll use is some kind of an attack, if they're able to install this equipment in the ISP, it is possible to redirect the encrypted connection to some kind of a proxy in between and collect data from there and from that proxy they actually connect back to Facebook, whatever is encrypted, the server, and as the name says, without the -- actually the users can notice that this is not actually valid anymore but -- any more but because of the issues in Thailand, it is not so much anymore, the knowledge of this, it is not that high. People are probably not noticing this. It actually happens. I just give you an example for a discussion of we're not saying that, like the government doesn't have any legitimate reason at all, right, to fight against a crime, right, and actually they need some data in order for them to work.

This actually demonstrates the mass surveillance. This is a problem. We cannot think of any legitimate reason to do this kind of mass surveillance. This attempts to do the monitoring by using social media platforms like Facebook, monitoring private communication on live chat apps and attempts to decrypt the encrypted data of coordinations. This shows us that they're actually trying to not do a target, but actually to do a mass one. This is something that needs to be discussed further, how the Committee as a whole will tackle this kind of issues.

>> SHAHZAD AHMAD: Thank you. Thank you.

>> I think this Facebook app, is it something that's original or was this like an original app and they have linked it, these pages to that page, the warning that shows on the Facebook app because it is made by Facebook?

>> No. No. It is made by the individual developers and we can trace back data.

In every Facebook app there's a URL, which is a API, and if you look at this graph API of every Facebook app it will show who is the developer and there are some specific information about the apps and there is a signature called TCSD which coincides with the name of the technology crime suppression division, which is one of the units of our police. After we show this to the public, TCSD, they came out, made a statement, yes this is actually the app that they do, but there is a legitimate reason for them to do that they claim because they actually like the public to be able to have a channel to communicate with them and further in the future if anyone has the foul they can use this Facebook or social media channel to communicate back to the police. This is a reason that the TCSD says that they have -- they have a social media connection in things like e-mail as well, so that they can e-mail back to the users who report to them then.

>> DONNY BUDHI UTOYO: I will be very quick. This is actually continuing what was mentioned before, this is from the citizen lab in 2013 about -- they found one of the surveillance softwares in Indonesia.

In March 13th there's a Citizen Lab, they released this update. I was in Toronto at the time for a workshop. For the first time I read this research. There's no attention enough from the media, in the Indonesia media, as well as from the government in particular, so when I was in Toronto at the time, I forwarded this research to media and tried to explain what is the surveillance and privacy, why is this important. It became hype on the media. There is headlines on the media, for example, Telecom and Biznet in talk, reported spying on the users, that's on the very top. Telecom, two of the biggest telco and Internet providers in Indonesia and also in the bottom Telkom, it says that we don't have spying servers. It is fighting on the media and there's no further actions even from the government, from the Civil Society to pursue the informations. On October, 2013 the Citizen Lab has sessions on the IGF, there was talk on the media in IGF2013 and talked about Indonesia and they found president spying application, so forth. Then it becomes hype again. For example, the top, it says there, what are they doing on the Telecom Biznet and in the bottom, the media says Indonesia governments are spying the Internet users. It is only one, two days happening and then nothing.

Maybe we can learn a bit from Indonesia. There is a famous act and regulation of who can do legitimately surveillance in Indonesia. There's a lot of regulations, a lot of institutions, so a bit confusing. Yes, we have regulations on surveillance, legitimate ones, but it is not so clear. It is a lot of regulations and bodies that can do surveillance.

Because of that, so any governments' organization, any government institution, legitimate that they're able to do surveillance, they can focus surveillance tools, even from the corporate enemies. You can see that in Indonesia, they have the software for wiretapping from the government, that was in October, 2013.

Because it becomes hype again in the media, wow, the military wrote something, saw something for surveillance, and this is the website from the minister of defense explaining to the public we don't buy spying software, surveillance beware, we're buying anti-spying software, anti-surveillance software to be installed and to secure the strategic compound, like the embassy, something like that. There is no further explanations. Okay. Okay. Then you do a good job. They're fine. We come back to IGF, why is there a lot of issues on surveillance, but it is still -- this is from IGF, one of our experts on cyberlaws, I see him specifically in Indonesia, that the privacy is not only protected, not only becoming awareness, why I consider this -- this is sort of the death of Facebook and Internet, in Indonesia, there is a lot of Facebook users and most are using a mobile and they don't -- they don't care about the privacy. They set is it all up with the Internet. You see on the right side, even if you can buy the surveillance tools online through the customer website in Indonesia, this is with everything you do on the phone, you can surveillance with anything freely. I know this is against the law, but practically you can buy surveillance software application and tools in Indonesia.

We think, okay, first thing, we have to create awareness among the people about the privacy surveillance. It is useless if we talk to the media. People don't understand the surveillance and the privacy. We do this workshop, we explain this, we create a discussion, we do campaigns with Mei and thank you to Shahzad, we can even then conduct the general lectures.

The biggest, most media then, the headline then, in June, the privacy protections on digital is really weak, it is now headline but they put someone else there. We also do campaigns through the civil media, we do Twitter, we have campaigns on surveillance. For example, during the first few months we create a twist first thing in the morning, we create the top -- the person, it is the surveillance address, this is against Human Rights, and it actually creates a campaign. We start this year to create a campaign on what is surveillance, what is privacy, what is important? Next year we'll do like this, communication and also with the press. I'll show you in 2 minutes why we have to develop the capacity of the press on this issue. Two months ago I was invited to an alliance to talk and share about privacy things. The night before I prepare -- only one hour -- I prepared a presentation and I randomly tried to find the media, the news, I find this, the ministry meeting on -- there was a traffic jam. I use this as an example to serve to the press at that time. I said, okay, if I'm a government, if I'm not happy with this media, with this information, then I can find the article on this myself. I know exactly who is the one that wrote the article and I can find that on the profile, on the profile I can also find his Twitter, her Twitter account which basically is locations. This is the press. This is the press from one of the prominent media in

Indonesia. With this locations, I can exactly understand where this -- the exact position of her and I can compare that oh, okay, this is not an office, this is the location of her home. I can pinpoint exactly where is the home. The sad thing is, I can also find the family, the child online, his photo, I can find also the discussions with friends. The most important policy in surveillance, in Indonesia, it is about creating awareness among the society and as well as the press workers and also the government.

Thank you.

>> SHAHZAD AHMAD: Thank you.

>> [Applause].

>> We now will go to the birds of a feather in the room and I'll request the panel to come here. If there are questions, we're now opening the floor on any questions and any contributions from the audience.

>> AUDIENCE: First of all, thank you for the wonderful presentations and the thoughts you have shared. Thank you to Citizen Lab and the work that they're doing to bring this to the forefront and the leaders like Shahzad that's taking it forward to the next level.

I would have loved to have that one -- that one chair should have been a government representative. That would be great. If there is anybody, I would invite him to join on the panel, but anyways, I wouldn't keep it open.

I just want to get into a government and want to learn about the physical surveillance and the -- when someone does a physical surveillance, when we install the camera, we don't usually question them. We're questioning government of seeing what we're doing online. I think the basis behind this is there's no proper segregation of private and personal life online media. I'm going into solution mode rather than problem statement because you have already talked about the problem. I would like to know from you what is the solution?

How can we make online life private and personal so that we can force government to only look at -- a public life and kind of get away from our private life, which we do in normal cases.

I would like to also mention when we talk about parental control, so we kind of propagate, we kind of promote surveillance by parents on their child. I was a panel member of child security, so we were actually promoting parents doing surveillance on their kids so that they know where they're going on the Internet so how is it different -- let's say the government is our parents. I would like to look forward to solutions.

>> SHAHZAD AHMAD: Anon, will you take this?

>> ANON CHAWALAWAN: Based on our experience in Indonesia,

we do approach very closely with the governments we believe that -- yes, we actually sit together side by side with the government to talk about what is the proper and right policy on the Internet of Things, of course with surveillance. The way that we -- we impress the government to think on the human right issue when they talk about this, we also develop the capacity from the Civil Society not only the Civil Society that focuses on ICT but other Civil Societies working on the human right issues, the woman rights and then they can -- the women rights and then they can take that from a regional perspective. For example, if the government released a bad policy on the surveillance, there would be enough mass, enough people, enough society that can say something and the media can easily understand what happened if also the media, the capacity is also developed. That's actually what they're doing.

Next year we'll have a discussion about the online data personnel, protection act. We don't have that time now, but next year we'll discuss it. We hope that all of the societies, Civil Society, private sector, government, they know what the issue is and then next year and then we can develop the good and proper regulation to handle the surveillance issues.

>> SHAHZAD AHMAD: You want to say something on this?

>> ARTHIT SURIYAWONGKUL: Can I, please?

>> SHAHZAD AHMAD: An update on the question, the children, the parents. Speak to that.

>> ARTHIT SURIYAWONGKUL: It is really interesting when you look at the parental control, there's one movie I have seen recently on the flight, it is called "man, woman, children" you know the theme of Juno? It is from the same director and I think it is called man, woman, children, it is about social media, about parents, kids and surveillance. Interestingly, the mother in the movie worried so much about her daughter, she installed all kinds of software in her daughter's phone, also the desktop computer, everything, just to track the behavior of her daughter. The question is if say if I have a kid, you also have a kid, our kid talks to each other, I survey my own kids communication but because my kid talked to Shahzad's kid, do I have legitimate power to also look at his kid? The communication, it is always coming in two parties or more.

>> Also the difference, parents teaching their children, on this side, it is different than state -- yeah. Yeah. That's also -- that's -- actually, this discussion has been used in a lot of countries to curve, you know, the open Internet and we have examples of that. If the United States acts at that level, yeah.

>> I can quickly wrap -- sure, I'm just trying to roll play and stimulate the discussion.

So that's one of the questions that was very interesting.

When you have the communications, it is not only the target, but it is everybody that your target communicated with. Even if you have a legitimate reason to surveil that target, do you have a legitimate reason to surveil everybody else.

The second point -- what is the second point? I have forgot. Okay. Okay. No. No. It is still -- no. Yeah. Okay.

From that movie, it turns out -- what's the end of the theme, it is really tragic, in the end one of the kids who knew her daughter tried to commit suicide because of the consequences of the parents in the movie, trying to very proactively protect her kids. Actually I would say that the mother knew that the kid would commit a crime, the mother, she's protected, she has done some measures against that boy to the point that the boy feels very ashamed and feels like he can no longer stay in society. That boy, he tried to commit suicide but actually the boy, he did nothing wrong. I think you get the data points, which is probably not -- not necessarily complete, but from this incomplete data point, you judge people, you prejudge people and this is a problem that's been demonstrated in a lot of movies like a precrime, these types of things. The problem of the surveillance, the mass surveillance itself, it is one thing, but the consequences of the mass surveillance, that's another thing, and that's a problem in itself.

>> SHAHZAD AHMAD: We have a question from here, and then that's the last question. That's it.

>> AUDIENCE: Thank you. Thank you for a lovely, informative panel.

One, Don, what you said about creating awareness, I totally agree. Remember John Oliver? He did a show about Edward Snowden and it showed quite clearly that, you know, most people he introduced, they didn't know Snowden. He asked surveillance, does it matter, in the abstract everybody said no. When he started talking about the infamous "Dick pics" then people said yes, it is personal information about me, then I'm worried about surveillance. I think that the answers are really there when we speak about surveillance in the abstract, people are like who cares, but then people think of -- say, think about your own personal information and would it matter to you if the government was looking at it, then they understand the rights, dimension, it sort of relates to them. That's one of the things as activists we have to do. I think related to that, I think sometimes -- forgive me, I don't mean to cause offense, sometimes as activists we're also a little sort of hard about it and we tell people you shouldn't be using Facebook, you shouldn't do this, you should encrypt, it is hard especially for younger people to relate to that as a defense and it is very parental, it is like don't do this, don't do that, stop everything, et cetera. A little of concepts in messaging.

Quickly, two, three other points, one is actually pertaining to this discussion, we have done research with teenager, they don't think of social media as either public or private, they think of it as semipublic and, of course, you know, to make it a private space we have -- we need intervention from platforms, from the technical community, from governments, but at their level they're using sort of a bunch of interesting tools, one is called stenography, it is writing in a code that they understand with their friends and their parents can't, they see parents as surveillance and the power question comes in there.

Similarly to that, I want to challenge you a bit if you don't mind, and say why do we think it is essential to even surveil our own children? What about digital trust? Forget orchids. What about digital trust, what about saying this is the Internet, you know, this is life, blah, blah, blah, navigate safely. Why is it essential to surveil? A thing we're finding now is we're having a culture of surveillance creeping in. Even in India a political party said to protect women being raped we have to put up 6,000 survey cameras in Delhi around toilets, there were a lot of rapes around that. There is a question between security and surveillance. How do we strengthen the security without everything being surveillance, surveillance, surveillance.

>> SHAHZAD AHMAD: We take this question as well and then we go to online questions.

Please.

>> Thank you.

I'm on the board of ICANN, but I'm asking this in my private capacity. I was interested in hearing about the presentations by Citizen Lab and about the intrusion and surveillance tools and I think the gentleman from Indonesia also briefly alluded to that.

My question is really about your opinion on who do we blame? Who is the bad guy here? Is it the vender of the tools or the governments that purchase the tools? To me the analogy I could draw is blaming the cigarette companies or alcohol companies for selling products that are in demand, are needed and needed is a strange word to here, but are in demand by the consumers and in this case the consumer is being the governments. Or it could be other parts that need these tools. Who do you blame? Do you blame the companies that make the products or blame the companies or the organizations that use these products?

Thanks.

>> DONNY BUDHI UTOYO: My short answer is, the ones to blame, it is if someone or somebody that knows it is not right but keeps silent. I mean, you blame someone that knows it is not right to do the surveillance but do nothing to change that.

>> PEN HWA ANG: I think my take on this is that there is a -- there was a generation of demand of survey lapse after the terrorist attacks of September 11th, right, it is interesting to pinpoint. From all of the various reports of what happened in the U.S. apparently despite a massive amount of intelligence, the massive amount of money spent, there is not one single incident they can point to where they used the intelligence to capture terrorists, there is not one -- using this intelligence, we're not talking about, you know, interrogation, whatever, but that's a good thing to point to. I think that after 9/11, it sort of conclusively points to the value of such information. If this is the position of the U.S., where they spend billions of dollars, what about the rest of us? Is it realistic enough? In a Singapore case they say that they have been able to foil terrorist attacks based on intelligence gathered but this is internal, we don't really know, there is no public testimony. You talk about the demand, and there is a demand on the part of governments and there is also a demand on the part of citizens. One thing about the U.S. airports, the reason they're inconvenient, the U.S. passengers, they're too secure, it doesn't stop terrorists, but it is so inconvenient, wow, we have don't something to help increase the security checks. Security checks are meant to give you a cover, a feeling of confidence, a confidence-being measure I would say. My take at the end of the day if you talk about who is to blame, it is us. We want to feel the security, you want to have confidence that something is being done by governments, despite the evidence to the contrary, something is being done to make us feel more secure is what I believe.

>> SHAHZAD AHMAD: Any or response to this?

Online?

>> Good afternoon, I'm helping with the on lean questions, there is a question, as the awareness of the surveillance will be influenced by how far people or citizens believe that privacy is important especially to see that data protection for each individual -- privacy -- as part of their human right, he's wondering how stakeholders look at this situation and if anything can be done to increase the awareness of society. He believes this issue can be solved but how long will it take.

Thank you.

>> SHAHZAD AHMAD: Indonesia.

>> DONNY BUDHI UTOYO: The short answer is yes, we have to

develop the awareness and capacity of the multistakeholders. We can only blame the governments or the grantor of the surveillance technology, but because somehow surveillance is -- the legitimate one, it can be done based on the transparent regulations. In Indonesia there's no regulation to do the surveillance on the Internet, for example. The more stakeholders now, it is efforts to think about this fundamental issues, the policy, the transparent policy and then we know we can understand which one is the privacy that's legitimate and which one is not. To understand that, yes. In Indonesia, we have to pose the Agenda of the privacy.

>> SHAHZAD AHMAD: We have already overran this session. Thank you for your presence here, for participating in the discussion. Thank you, panelists, you were very generous in sharing all of the good knowledge that you had. Thank you.

Thank you, Irene. Thank you, Donny. Thank you, all.

A round of applause for our --

>> [Applause].

>> SHAHZAD AHMAD: Essentially it is not surveillance or the tools, but the real layers on the ground that will bring security and that will help us with the Internet for all of us.

Thank you, again, all of us for this.

***

***