FINISHED FILE

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

JULY 28, 2016
ROOM 401
11:00 A.M.
WS 67
INTRUSIVE SURVEILLANCE TECHNOLOGY COULD BE JUSTIFIED?

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

***

***

>> We are checking remote participation devices, so please give us a few minutes.

>> Hello.

>> Surveillance by technology. She does on the communication device is continuously recorded and transported over to the person conducting, or the agency. These forms of surveillance, in some jurisdictions, have been used and have been justified as an extension of traditional surveillance without any legal reform or without any discussion on whether this new type of surveillance should be allowed, and can be justified -- or can be conducted following the normal procedure. In other jurisdictions, discussion is going on right now whether this type of surveillance should be even allowed.

For instance, the U.S. is right now conducting discussion on (inaudible). Judicial approval of surveillance. And they are talking about the need to revise FICP for that purpose. So, we have a wonderful group of panelists who can shed light on this issue. (inaudible) ICS. The software developed -- sold to strategic intelligence agencies around the world, like NSA, FBI, or NIS of Korea, or MI6. We don't know whether those software were actually used by those agencies. We don't know for all of them, but that has been -- for

the internet society, Hong Kong chapter, and by Internet Governance Forum, APrIGF, Multistakeholder Steering Group, and Councilmember of the Forensic Society.

He has been a Technical Adviser to Hong Kong government. So, he will also participate. And on my left, we have someone who has followed closely the Hacking Team fiasco, and there's a fiasco in Korea because NIS, National Intelligence Services of Korea, has been heavily implicated with (inaudible). Hacking software against its own civilians. Then we have a development and media professional with a focus on research and advocacy in human rights, democracy, regional peace, and she has worked on digital rights and violence against women, and has done research on -- researched on the same issue with Bytes for All.

And we have the cofounder of -- joining us remotely from Delhi, India. He is a Counsel with Software Freedom law center. It's a nonprofit organization working to defend netizens' freedom in the digital space. Without further ado, we'll start with a presentation of Byoung-il Oh, he was the organizer of this workshop. And on the first round, I'm thinking we'll -- each speaker will speak for seven minutes, probably starting with a more descriptive presentation of what's going on in the world, and in their own jurisdictions. And whatever they cannot fit in those seven minutes, we'll do a second round of speeches. So, do you want to begin?

>> BYOUNG-IL OH: Thank you. My name is Byoung-il Oh, and I'm very happy to be here and discuss this interesting topic. After Snowden revelation, serious concerns on mass surveillance was raised by civil society, technical community, and even government in the U.N. But apart from that, we need to discuss the problem of intrusive surveillance technology like hacking tools, which is installed surreptitiously on target computer and monitor and gather various activities and information on the device.

And so we need to discuss whether those kind of technology (inaudible). And intelligence purpose -- methods used by law enforcement agents before, and could affect other users who are not suspect, and even the security (inaudible). So, first, I'd like to brief you on the case in South Korea, before Hacking Team was hacked, and the materials -- it was reviewed by the data that the intelligence studies of Korea had used the product of Hacking Team, and remote control system since 2012, which raised a social concern in South Korea.

Of course, Korea is not the only country that had used this. There were law enforcement or intention agency of Singapore, Malaysia, and Thailand. As you know, Hacking Team is not the only company who developed and sold these kinds of surveillance technology. So many other countries are also a customer of this technology. It penetrates the target device by infecting it with malware, malicious code by

sending fishing email, or SMS messages which could attract the target's attention, or using vulnerability of application.

Actually, spyware could be installed on various operating system, including Android, iOS, and Windows. When it succeeds to penetrate the target device, it could collect personal data of the target including call records, contact list, photos, and other documents, and intercept phone calls and messenger exchange. It can even control microphone and camera remotely. It was known that NIS of Korea had bought 20 license, which means it can surveil up to 20 targets simultaneously. The slide is the snapshot of an administrator console used by NIS.

In the picture, you can see in the red box, NIS is monitoring 17 targets. The picture on the side shows which function is provided. The meter is for what purpose, an IS had used this tool. NIS admitted it had used RCS and said it was for analysis and research, preparing for intelligence work against North Korea and other countries. And it had tested it against the North Korean agent. However, the link between Hacking Team's staff and NIS agent shows the possibility that RCS could be used for monitoring nationals.

This is the part of the mail between Hacking Team staff and NIS agent. There are some circumstantial evidence. First, NIS demanded to Hacking Team specific capability for monitoring newly released internet model of some smartphone, Galaxy S6 or S6 Edge. Second, it also asked Hacking Team to support interception function of line, which is the most popular messenger apps in South Korea. I think it's very hard to imagine North Korean agent used this without considering security.

Third, another demand of NIS was the capability to evade the detection by antivirus application, the most popular antivirus application in South Korea. Fourth, NIS had asked Hacking Team to make hundreds of fishing URLs and spyware. Among them, there were fishing URLs which seem to target nationals such as URLs to food blog in popular site, or cherry blossom festival blog, and information site. Among the infected document, there were alumni of the University Engineering Department, and a male which impersonated journalist.

Yeah. This is the infected document, NIS. This is the mail NIS asked to hacking team to implant the malware. And this mail impersonated a journalist, a newspaper journalist in South Korea. In spite of circumstances which raised out, decisive evidence has not been found. And NIS didn't disclose detailed information how it had used RCS, even to the National Assembly, saying that it is protected as confidential. Actually, I don't know NIS had really used RCS for monitored nationals, but even if NIS didn't surveil nationals yet, there's something we can point out as obvious problem based on the fact.

That is, there is no oversight over NIS. As NIS admitted, it's obvious that NIS had used RCS since 2013, but anyone didn't know that NIS had used RCS until Hacking Team's internal material was revealed. The Intelligence Committee of the National Assembly is the only oversight body over NIS, but it didn't know either that NIS had used RCS. Even after the fact was revealed, it couldn't investigate for what purpose and how NIS had used RCS. Who knows if NIS is using other hacking tools as well as RCS. And who can be sure that NIS would not misuse those power?

Actually, NIS had a very bad record of misusing its power to monitor human rights activists and journalists and politicians, in internet politics. So I stop here and talk about the risk of this kind of intrusive software later. Thank you.

>> K.S. PARK: Thank you. Next, actually, they're asking me to put something right after him, because he will also talk about Korea. Then I realized you don't want to hear from three Korean speakers in a row.

(Laughter)

>> K.S. PARK: So I'll have Chester go next, and this is more proper, because Mino will be talking more about how civil society responded to Hacking Team's scandal. So that's more a proscriptive as opposed to descriptive. So, we'll let Mino go probably in the second round, that may be more appropriate. Anyway, Chester, you're up.

>> CHESTER SOONG: Hello. Good morning, everyone. Well, when Byoung invited me to this session, I agreed right away, because privacy and surveillance is what I believe very strongly in heart. But it's interesting, this topic, when I think about it more in detail, because I've been spending most of my time in information security and working with the police on cybercrime investigations. I help them with digital forensics, system development. But then I also work at the Office of the Privacy Commissioners in Hong Kong, just last year. So I'm kind of like far left and far right. (Laughter)

And I'm even involved in a startup that is developing -- or has been developing cyber intelligence tools. (Laughter) You know, right now. So -- well. But, anyway, I'm with you. (Laughter) That's why I'm no longer working for the DBA. Anyway, I just want to bring up one thing first. Can I have the next slide? Oh, sorry. Yes. Right. Now, a lot of people -- or, you know, governments, law enforcements, when they tell you they need to do surveillance, they have to have the capability for surveillance, two very common reasons that they have would be, you know, crime prevention investigation, counterterrorism, things like that, which I agree with, you know, a lot, except that is it really as effective as they claim?

I mean, it's a good tool, but -- you know, I mean, the reason I cited those two examples, those very recent examples of terror

attack -- now, I choose my word very carefully. I don't want to say they are like terrorist attack, because officially, the authorities still have -- still, you know, have questions of connecting them directly with, you know, any terrorist group. One has claimed responsibility, or organizing or involved in the Nice attack, but the point here is these two individuals who launched the attack were completely off the radar of security forces of the intelligence community.

So, does this mean that -- if you talk about surveillance, does this mean that every one of us has to be on the list -- has to be monitored? Because, you know, I mean, I'm sure a lot of us in this room are not on the list, you know. Maybe I am. I don't know. But I just don't think I'm significant enough to be on the list. But really, so this raises an issue, how far this surveillance effort or the authority given to the law enforcement or intelligence community should be? Sorry. Next. Now -- yeah. To bring it back for the audience, what do you mean surveillance?

Now, the topic here we have is intrusive surveillance. Like someone was saying, every surveillance is intrusive. To me, I slightly disagree with that, because, you know, for us, for me, who know a little bit on the intelligence research, we do get a lot of information from just open data on the internet. Really, we do not have -- I mean, for example, I think the bomb attack in Paris last year, they were able to actually identify at least two of the attackers based purely on open data. So -- but, anyway. You know, we -- the point here is, you know, we have surveillance.

But the point is, we need to know that there are, like, secret surveillance -- something that is, you know, completely off -- well, not completely -- but mainly off the system of oversights. You know, things that -- activities that were done by the intelligence, you know, agencies that are not really, you know, monitored or questioned, or preapproved, you know, to the level that we as the citizen would be comfortable. So, information that are collected, you know, about people, by these services, could be used anywhere or by anybody. And I think recently I was watching the news about the Catalonia province in Spain was trying to launch another referendum for independence from Spain, maybe next year or in a year or so.

The relevant point here is there was an allegation that they claim about the current interim Prime Minister doing surveillance, and also using information that they collect on the opposition in the Catalan region to discredit them and attack them on that front. Now, whether that's true or not is out of our context, but there are some other things that could be used. And, of course, you know, I guess maybe we can talk about jurisdiction, but in Hong Kong, sadly we don't have much to say in these regards. I mean, especially if

you -- if any of you have heard about the incident about the Chinese bookstore, they were -- well.

We say they were taken, but they said themselves they went to China voluntarily, in their own ways to help the investigation. I cannot think of anything that's more intrusive than that. (Chuckling) Than the surveillance that we are discussing here. Now -- so, go back to the slide about, you know, I guess two of the most famous laws that we have globally would be I guess the -- especially after the Snowden revelation was the FISA and the USA PATRIOT Act. I don't want to go into detail, you can search on open net. But the point here is it gives the authorities a lot of power in terms of surveillance, both physical and digital, online and offline.

And, of course, after the revelation, President Obama tried to, you know, revamp or -- on the FISA act. But we all know that what he proposed wasn't really satisfying to the community, or to the liberal community. So, it's a great concern for us, although these laws have Congressional oversights. But I think we question a lot on how this is going to be. So I think I will stop here for a moment, and, please.

>> K.S. PARK: Thank you. Just for clarification, what we mean by intrusive surveillance doesn't have to be secret surveillance. By secret we mean not letting the person being surveilled know that he has been surveilled. But most wiretapping laws -- if the country has a wiretapping law, usually the person wiretapped receives notification that he has been wiretapped after the wiretapping has been completed. So in that sense, it's not considered secret surveillance, because people with given notification later. But when we talk about intrusive surveillance, it's the method of surveillance.

By intrusive, what we mean is hacking into the communication system of the user and planting certain software that will do the job that in the past has been done by human agency. Even that, after the surveillance is done, you know, people can receive a notification -- theoretically, they can receive notification later that, you know, their devices have been infected with malware. So just a point of clarification. You're next.

>> Thank you. Hi, everybody. I'm probably, maybe, like, go a little bit further as well, like, on, like, why. Why this technology has been of interest of more and more governments around the world. Yeah. So, probably, first of all, maybe back to the basic first. Like, how to actually -- when we're talking about the data on the internet, or any computer system, basically, we have two categories of the data. The first one we call it data at risk. It's data that sits inside a device, right, waiting for the processing or whatever. In your USB stick, in your CD ROM, in the devices, this is all the data that we put in the category of data at risk.

It sits there waiting to be processed or transmitted, right. But it's not going anywhere yet, so that's why we say at risk, right. Another category, it's data in transit, right. So, when we do a communication, right, we're talking from one device to another device, one end to another end. The data that's transmitting in between these two devices, we call it data in transit. Most of the communication surveillance like before this kind of software, RCS, whatever, most of the time is -- also when we're talking about wiretapping, we're talking about the surveillance of data in transit.

So the data in between. Because of the popular of communication encryption, more and more networks, Facebook, YouTube, Twitter, especially after the Snowden revelation, a lot of internet users are now aware of the threat to the privacy. So more and more of the service provider consider to use this encryption. Like, for example, SSL or HTTPS, when you use a web browser, you can notice that there's a green padlock at the address bar. That means the communication between your device and the server of that service provider is protected, right, by the encryption.

With this encryption, it's made more difficult for anyone to actually, like, get in between and read your data in transit, right. So, one of the way to get around this -- if the decryption of the data, it's difficult, why not just go to one of the ends and read the data before it got encrypted, right? So if the data in transit -- right. So I would say this is one device. And this is another device, right. And this is, like, a link, right, communication link. It used to be the case that they do interception at this point, right?

But because it's got encrypted, it's getting more difficult. So why not you wiretapping it, get the data, do the interception at this point, or at this point instead, right? So when we talking with the RCS thing, it mean that, like, when your device -- right, your mobile phone -- got infected, they actually read your data before it got encrypted and sent out of your device, right. This is why this kind of measure is getting more and more popular, because, for example, governments and also all those, say, bad people or hackers, whatever, right, it's difficult to get in between.

Back to my slide -- thanks. Maybe next, please. And the problem is here that -- okay. This is from Thailand, but I think, like, this kind of problem, like, it's more, like, in a lot of places in the sense that, like, yes, a lot -- we -- in a lot of countries, we do have a law that allows authorities, right, to get access to the information, to collect the evidences, right. If there is a reasonable belief, like maybe the criminal activities may occur, right. But the thing is that the language there is not really that clear.

For example, when we're talking about granting the official to have the power to acquire the evidence, we're not sure how to interpret this, right. It maybe used to be the case that it's talking

about intercepting data in between, in transit. But because of the language, it's not so clear. Maybe it's also allow the officers -- maybe, I'm not sure -- maybe allows officer to also plant something in your device as well. And I think because of technological -- there is a necessity to have a more clear, more precise language in the law, right, because in the past, maybe this thing, there's been no differentiation, right, 20 years ago, 10 years ago.

But right now there's some differentiation and the consequence is different, as K.S. Park said, right. The interception of the data in transit many times, it's probably needs some cooperation with service provider or whatever, right. So maybe there are some traces that you can trace back whether the communication has been intercepted or not. You can check it back. Maybe you'll not know it right away, but later there will be some notification so you will know about that. But in comparison, in contrast, if your device got planted, the interception will be more or less continuous.

So there's no point of time to say, okay, we should send a notification to the user that there has been a wiretap that intercepted, because basically, there's no end. The interception is just continuing as long as that piece of software stay in your device. Maybe I just go quickly. I can do this. Thanks. Right. I'll just stop at this slide before pass to other people and just come back to the comparison with our existing law. So, at the moment, there are eight things -- eight category of powers that allow authority to do.

Three of them probably related to this surveillance, planting something in your device and continuously copying, right, or collecting information off your device. The first one is the copying of the data off your device, inspecting or access. Maybe it's in your SD that attach, the ROM, whatever, as long as it can be accessed from your device, it has power as well, according to subsection six of 18, right. And also the last one that's probably related is the recording, right. So if your data is encrypted in your device, right, now the data, for example, iOS, probably since iOS 8, and Android 5, maybe, user has option to encrypt everything in that device, right.

So this will also allow them to -- the authority to get that as well. I will just stop it here and, like, come back later. Thanks.

>> K.S. PARK: Thank you. Actually, section 18 of computer-related crimes act is, from legal point of view, that's the most comprehensive I've ever seen, giving powers to the state, in terms of the breadth of the variety of actions that the government can take. Anyway, is Prasanth ready to go?

>> Yes, I can hear you. I cannot see you.

>> PRASANTH SUGATHAN: Okay.

>> K.S. PARK: Why don't you start? They can get your visual later.

>> PRASANTH SUGATHAN: Thanks. So, good morning, everyone.

>> K.S. PARK: Good morning.

>> PRASANTH SUGATHAN: It's a pleasure to join all of you remotely. I would've preferred to be there in person, but this is the next best. Thank you all for inviting me to be on the panel. So, to start with, my focus will be mainly on the intrusive technology and how it works mainly in India. We did a study on privacy and surveillance, and the laws which relate to that in India. And while we were doing the study, we were at a few conferences interacting with people who are involved in this, mainly from the industry. And this was before the team disclosure. Can I have the next slide, please?

>> K.S. PARK: Wait for a second. Okay.

>> PRASANTH SUGATHAN: At one of these conferences, we met a person who said he works for the government, an independent contractor. He said he works for various government agencies. And modus operandi, he said, is the same with us, the Hacking Team tools work. Once they identify a target, they try to get a project in plan, get the malware implanted, and try to access their system. This was a revelation for us. There is no permission in the Indian law as far as we know by which they would've done such a thing.

There are certain procedures for telephone tapping and wiretaps, or internet monitoring. The systems and processes are similar. But here, without any procedures, without any safeguards, we had various government agencies relying on private things. And that was the most important part. It was not that they were doing it, they were relying on private parties to get it done for them. So, the main problem with all this intrusive technology is that they rely on the backdoors of software. So any operating system, any software that we use, whether it is Android, Windows, or Apple iOS, whatever it is, they rely on the back doors, the weaknesses of the software, to gain access.

And once you have a back door, it's not just -- agencies who can get access. And this could be exploited by anyone. That really is a major issue, and it's not just -- and specifically, the case that I mentioned, when you have private persons who are doing it, and not just the government agencies. And that increases the problem. And then came the Hacking Team disclosures, which showed that there were various central government agencies of the Indian government and various state governments -- with our system, there are various state governments -- who, again, have the power, in the case of wiretapping, they have the power to tap, let's say -- even they were doing it.

So they were in discussions with Hacking Team to gain access to their systems, to buy their systems. So this was information which was on the disclosure, out in the open now. The problem here is if you look at, let's say, a person trying to access a system without the permission of that user, well, that is a criminal offense. And here, we have government agencies who were hiring private persons to do that for them. And we definitely don't have a law to deal with

it, in the sense we don't have a law which allows the government to do something like that.

Can I have the next slide?

>> K.S. PARK: You've got it.

>> PRASANTH SUGATHAN: Okay. One problem that we have in India -- and which is being intensely debated now -- is that we do not have a right to privacy explicit in our constitution. The courts have interpreted the right to life and personal liberty, which is there in the constitution in article 20, which is a fundamental right, to include the right to privacy. But, we had a recent case in which the highest law offices of the government told the Supreme Court, the highest court in India, that there is no right to privacy as far as citizens already concerned, and it is not explicitly in the constitution.

And now, the matter is before the constitution bench of the Supreme Court. And we really don't know how this will go. But I hope that we have a serious objective, whereas the Supreme Court passes the right to privacy. Can you move the next slide? As far as the surveillance laws in India are concerned, the basis for all these laws are essentially a law called the telegraph act, and then the IT Act, and various other procedure rules which cover that. I don't want to go into details of that, but the problem with all these laws are that whatever safeguards you have, and whatever orders are passed, everything is done by executing.

There is no judicial oversight of any of these actions. And Professor Park was mentioning about how in most cases, in most jurisdictions, where there is a notification which is given to the person who was surveilled. But even in India, that doesn't happen. You never know whether you were the target of surveillance. And consider the case -- in the case of something like intrusive technologies, you don't know. Even in the case of, let's say, wiretapping, you don't know. This is something which is totally outside the realm of law the way we have it in India.

So, I mean, what kind of solutions do we have? Now, I'm trying not to take too much time, so my last slide. Can I have the last slide? The 12th slide. It's the last slide. So we need to realize --

>> K.S. PARK: You want to see the very last slide?

>> PRASANTH SUGATHAN: Yeah. The last -- the 12th slide. Yeah. Thank you.

>> K.S. PARK: This one is titled "solutions."

>> PRASANTH SUGATHAN: Exactly.

>> K.S. PARK: Okay.

>> PRASANTH SUGATHAN: Okay. So the question here is, what do we do about it? Do we have an answer to such intrusive technologies, what governments do? Let's say, with the support or without the support of law? And that is where we need to help people deal with

everybody, we are all gathered here, to work together on solutions. This will not come only from the law. This has to come from technology also. We need domestic laws which will deal specifically with it. We will need international cooperation. We need to ensure that there is privacy by design, because the root cause of all of this is trying to exploit the back doors in various softwares, and the flaws in various softwares.

That is where we need to make sure that whatever software is developed, we don't have back doors in them. And that's what many governments are trying to say we need back doors to gain access, but this is something that we need to ensure that is prevented. Thank you. We'll get to details later.

>> K.S. PARK: Thank you. Prasanth, stay on. I know that you have these interesting diagrams, and you will have a chance to talk about them in a few minutes, so stay on. Okay. Next, Gul, you're on.

>> GUL BUKHARI: Thank you very much, and hi to everybody. I'll give you a little bit of overview of what it is like, the situation in Pakistan, and it almost seemed like every one of you has spoken a little bit about Pakistan. So the situation seems to be very similar almost everywhere. This country is about close to 70 years old. Half of its years that it has been in existence it has been ruled by the military. And the military has been very, very powerful, even during times of democratic rule, because behind the scenes, it rules most of the powers.

And surveillance or espionage, etc., has traditionally been the strongest by the military, and its establishment, we call it. It's happened forever. The tools used to be different. There used to be wiretapping, very crude type. But as technology has moved on, of course they have been buying more and more sophisticated tools. And there is -- it's getting documented all over the world with Snowden's revelations, with the hacking -- sorry, Hacking Team, etc. So, all over the world, it's getting documented.

I'll jump straight into what Byoung described as the technology. Back in 2012 or 13, Citizens Lab did some work in Pakistan, some research, and found that this software, FinFisher, they found it to be using Pakistani infrastructure for its command and control. So we have evidence that as far back as -- and FinFisher is very similar to the technology Byoung described. Very quickly, to recap, it is intrusive. It works through download. Once you get infected, it can read down to every keystroke. It can turn on your camera without you knowing. It can read the emails. It can access files, etc., etc.

So it's very similar technology. So, this is back in 2012 and 13. Then, connecting with Chester's point, given the fact that it was being used way back then, or was discovered way back then, in 2014 we had the most horrifying terrorist attack on the school. And over a hundred and, I think 40, children were killed. Now, this is one other thing I think which is slightly different about Pakistan.

But first I'll finish my point. How useful was that technology in averting a terrorist attack inside the country?

And that is only one example. We've had many. We've had them on ethnic groups or religious minorities, like they would attack a church, where maybe over 100, 120 Christians died, so on and so forth. It is really not preventing that. But now, very recently, in May, there was news. And that is the only way we can find out. It's a U.S.-based malware protection company called Fire Eye, and according to them, it is the use of a highly innovative surveillance software, CDOR. And according to this report, the malware has been used to supply on political dissidents within Pakistan and the Indian military.

So in this case, we know about the targets as well. With FinFisher, we didn't know. This particular report tells you about the targets -- the kind of people that it has been hitting as well. So, it's been used to spy on political dissidents in Pakistan and the Indian military, and has been reported to be extensively using Pakistani infrastructure for command and control, which indicates a Pakistani origin sponsor. And according to the same source, a cybersecurity firm identified the malware, or malicious software, as a robust surveilling malware called CDOR, often initially delivered to a target computer system by a downloader.

It then creates a back door to the victim's system and it can interact with the file system and so on and so forth. So this is the second example. Obviously, it's completely outside of the legal framework. It's already being used. We don't know -- with this one, yes, who is a political dissident? That's a very general term. But from our work on the ground and things that we have experienced and seen, normally it is human rights activists, political opponents, or the party in opposition to the one, maybe, that the military has put up.

It's the people working on the India-Pakistan peace process, journalists, and politicians in general, judges. So this is a tool. And I'm not saying that only the intrusive technology is aimed at these. Traditionally, all sorts of surveillance was conducted on these groups of people. Hilariously, and whilst Chester pointed out that, you know, governments use this as an excuse to fight terror or to prevent crime, or etc., etc., the best part is that we have a long history -- we've been in the middle of a war for the last -- God knows.

It started in the late '70s when Afghanistan was invaded by the USSR. So we had our non-state actors participating in that, if you understand that. And it created -- (Chuckling) And since that time -- and then the USSR left after a long-drawn, bloodied nose. And then 9/11 happens. But between USSR leaving and 9/11 happening, the non-state actoring kept going on and on and on, and these groups

really exploded in number. And then, obviously, they were -- you know, when one war was over, they were kind of directed towards India.

And then something happened, and they were told to come back -- don't go to India. So they started targeting ethnic minorities in Pakistan. They have to do something. You created them, yeah? Sorry, how much time do I have? Okay. So the thing is that these actors, the terror actors, they still are working on the ground, pretty much under the watchful eye of the state. But these various tools are being used. So in the second round, I can come back to the legal framework that we are about to introduce in the country. And that would be very relevant to what's going on, because right now the surveillance is completely outside any legal framework. Yeah? Thanks.

>> K.S. PARK: Thank you. So, we have our last speaker, Mino. But because he's going to talk about civil society response, right now we'll do question and answer just for ten minutes, or five to ten minutes. And then we'll have Mino speak. And then give other speakers a chance to make up for what they missed in the first one. Any question or comment on what has been presented so far? None? Okay. All right. Excuse me? Well, I think that is a question we are trying to resolve. Apparently, much surveillance is going on already under the existing laws.

The Thailand law, section 18, seems very comprehensive. But looking at the text, it's not clear whether it specifically justifies surveillance. I haven't seen any law that specifically authorizes surveillance. I think what's important is not whether it's justified by law, or whether we as a multistakeholder should let it happen. Next? Okay. I think she was next, yeah. Go ahead.

>> AUDIENCE: Hi. So, I have a comment and a question. So, to me, it feels like surveillance is a double-edged sword. So in some instances where there is -- I'm from Pakistan. So in the context of Pakistan, it's useful also to tackle terrorism, but on the other hand, it can be misused widely as well. So, we speak about the attacks that did take place despite all the surveillance, like the APS incident where 140 kids were killed, and other incidences. But there must be instances that were stopped and prevented because of surveillance that we don't know about.

So, I'm saying that we see the things that do happen, but we don't see the ones that were prevented. So, yeah. To me it's like, somewhere, like, you can and you can't justify it, so.

>> I don't see it as a double-edged sword at all. I see it as a completely single edge. There is evidence, studies have been done for Europe and the U.S. where this kind of surveillance or mass surveillance has been going on for a long time. And yet incidents happen, which you call, these are the ones we see, what about the ones we don't see. Is there any evidence that this kind of intrusive surveillance has stopped a single terror attack? Without evidence,

we cannot claim that. In fact, it would be the best justification for governments to use it if they could provide evidence.

But that's -- I am sorry to say, BS. You keep claiming as a government that you need to do this, and you have not provided a shred of evidence, right? And what we have evidence of are human rights abuses that governments do during this. Look at what happened in the Arab Spring. They were surveilling and using different technologies and going and finding dissidents and political activists for the Arab Spring. We have human rights activists who were targeted. Now, I can't say exactly which technology, whether it was intrusive or slightly older.

In Pakistan, we have -- everything is connected. The NDRA database, the national identity database, it has your biometrics. It is now linked to the safe city project, 1800 cameras installed in a small town, the capital, which has face recognition software installed in it. It's connected to your ID card, which is connected. You can't get a phone without presenting your ID card. You're being -- common citizens are being surveilled, and every month there are so many incidents happening. So that's where I'm coming from.

>> K.S. PARK: Okay. Next.

>> I notice that you talk about having a process on the use of this information that might or night not be useful for national security. So I'm talking about committees, law, and processes. Do you folks have any idea of what kind of processes would be helpful in this kind of situation? Thank you.

>> K.S. PARK: Okay. Let's take that question after the second round, because some of the panelists may have answered already. Yes. You will be the last question on this round.

>> AUDIENCE: Thanks. John from Electronic Frontiers in Australia. A couple points. Firstly, the Australian Parliament passed a law, the Intelligence Act in 2014 which gave our domestic intelligence agency the ability to add, delete, or modify anything on the computer of a suspect. That's pretty broad. And it also redefined the definition of what a computer is in such a broad manner that it quite literally could be interpreted to essentially apply to anything on the interpret. That's pretty broad and sweeping there.

We know that, you know, technologies like this were used. We know that they were a part of Hacking Team. We know that some of our state police have used FinFisher and other things as well. The other point I wanted to make is about the likelihood that foreign intelligence agencies are working together and sharing data. We know this is happening particularly within what's called the Five Eyes Alliance, Australia, New Zealand, the United States, Canada. We know that there is surveillance going on where they are essentially bi-passing the domestic laws by getting a foreign agency to spy on their citizens.

So the GCHQ in the UK spies on the U.S., they're sharing around, we know that's happening. That's a close, formal alliance. I'm sure the U.S. and others are doing similar things with other countries that they're close allies with in certain circumstances. So, part of the challenge that creates, of course, is that it doesn't matter what your domestic laws are, because it's just going around them.

>> K.S. PARK: Thank you. Mino, it's your chance to speak.

>> MINO CHOI: Thank you. Hello, this is Mino Choi from Korea, and it's an honor to participate in the discussion here. First of all, I'd like to start with the Open Project, a result of collaboration within Professor Park, and Mr. Oh, and the activists. So, after that, there were laws -- organizations. International, and various other organizations, which was for detection on Windows PC. But it also indicates that Hacking Team -- for phones which at the time -- of users in South Korea, too. So -- find the victims -- we decided to develop and publish an open source connection tool.

As someone discussed earlier, intelligence -- were able to -- the victim's phone, largely by either taking their -- application and email, or other methods to make victim go to malicious website, or simply control such as Wi-Fi or ISP in order to send the application secretly. Developing detection tools -- to build -- implication from emails. The engine -- and to see if there is any implication. We know that -- simply use the function in order -- all the threats on their notification of the victim's system -- compromise.

So -- chance detect the malware while the malware is still installed, which would be the case that the user -- victim. However -- servers -- also suspect additional chance to detect victims which -- attack -- due to lost connection. Application successfully -- about a year (inaudible). Concerned citizens -- followed by United States, Italy and France. Also, University of -- application -- signature to our database. The result is that we could not find victims by the application -- detection -- identify -- service -- intelligence entities. Also, with this experience, I also want to point out that -- is collecting -- is privileged -- control the system forever.

Back door -- where it's easy -- terms -- modified version in order to keep the back door open. In other words, once you get your system compromised -- regardless -- system restore -- get another one. Furthermore, the previous case is -- most of the time -- compromised -- try to restore. This is problematic, says -- surveillance technology -- intelligence agencies can still control your system if you don't replace the system. The system has been compromised. And there are various ways. Not only -- specifically -- surveillance tools such as Hacking Team -- depend on every day.

Intelligence because -- yesterday -- forgotten. Data -- and commercial entities get support from government entities. The data of the victims is still on the table. Servers -- services -- ISPs, installations, all of that. Sometimes -- vulnerabilities -- doesn't get fixed for decades. Some would argue that this is necessary in order to prevent terror attacks or keep safety, but in the world of the internet -- explore these vulnerabilities can be exploited -- not just intelligence entities. So, in fact, the fear is that, I believe -- inside the security -- to have better security.

>> K.S. PARK: Thank you. So, starting with Mino, I'll give other speakers a chance to speak again, focusing on what to do and what should be done. Two minutes each.

>> I have worked for advocating human rights for over ten years, but in principle, I don't deny the necessity of some level of wiretapping. But actually, I can't agree on this kind of experiment -- using this kind of surveillance technology. For this explanation, I refer to the joint submission by Privacy International Open Rights Group. Because it articulates the point very well. And I fully agree. The first risk is, this technology is too intrusive in the small smartphone. We can make whole profile of you. So -- and there are many materials and information which is related to certain crime.

And second, when we deal with this, it's very important to keep the chain of custody. But this kind of technology can . . . Yeah. Can compromise the integrity of the evidence. And finally, I think it's very unethical for government to use this kind of technology, because it can compromise the security of the users of -- who are not suspect, and even the entire internet. So -- but even if this technology would be permitted at all, it should be allowed in the very strict conditions. So, again, I refer -- oh, no.

Again, I refer to the submission of Privacy International and Open Rights Group for the necessary condition. I will not explain in detail about this in consideration of time, but it deals with ten conditions, such as the -- it should be allowed in a very limited -- when there is a concrete evidence -- concrete probability of -- to -- of a serious crime, or the relevant evidence is highly likely to be obtained, etc. But I'd like to point out some other important point first. This condition should be articulated in the law very concretely.

For example, in Korea, there is a law which regulate wiretapping, or which regulate the collection of metadata, but there is no law which directly regulate this kind -- the use of this kind of technology. And as mentioned before, in other countries also there is not much -- there is not a law directly regulate this kind of technology. Second point is to balance the necessity of using this technology

and privacy and security of citizens. I think there is no absolute criteria to balance them. But it depends on the situation.

For the consideration of the balance, I think one of the most important point is the trust on the investigative or intelligence agency. In relation to that, in Korea, NIS of Korea has no trust on them. You cannot trust NIS of Korea. They say, "we have changed, trust us." But trust is not gained by just promise. Trust could be gained by only effective oversight mechanism. So, I think these two conditions -- first, this law, and another is effective oversight mechanism is essential. Thank you.

>> K.S. PARK: Thank you. Chester, your two minutes.

>> CHESTER SOONG: Can I have my last slide? Yeah, the last one. The last . . . Sorry. Okay. I hope to provide a bit of an answer to the gentleman's question earlier about, what are we going to do about it. I think the first question is, if surveillance is justified. I think it should be asked. Like, well, who can justify this? You know, who is going to, you know, decide this is -- we need it, and, you know, for every single effort in surveillance monitoring, citizen, who is going to review that authorization decision, you know.

And then who oversees this afterwards. You know. And, you know, whether the citizen is being -- you know, has a say, or informed of this, right. I mean the whole process -- I mean, the answers to all these questions, hopefully, would form some kind of, like, a sense of trusted process, you know, like Mr. Oh was saying. The other thing, this is an official -- not just for advocates that, you know, we want our privacy to be respected, observed, and, you know, protected. But it's also, you know, beneficial, I think, for the law enforcement intelligence communities to do the work.

Because if you don't get the trust from the community, how're you going to get your information, how're you going to get cooperation? And to be frank, you really, for law enforcement, it is impossible -- it's almost impossible -- for them to solve a crime, to apprehend a suspect, really, without any help from the community itself, or from the citizen itself, you know. You can imagine if everybody from the community act against you, the law enforcement, investigating a crime, how difficult that would be, right?

So, really, I think it's really unacceptable for, like, unaccountable surveillance, okay. And I think we need clear legislation to give limited power to the law enforcement to do their work. But, you know, for the citizens, you know, we need to have it with oversights. Yeah, thank you.

>> K.S. PARK: Arthit, your two minutes.

>> ARTHIT SURIYAWONGKUL: Thanks a lot. I think there's two parts, right, that I'd like to say. So the first one is -- do do, da da da. And I cannot reach -- I'm sorry. But, yeah, thanks. There is some helping hand from somewhere. (Chuckling) Can I go -- sorry. Yeah. So,

like, the first part, the law. Another one is the technology. I will probably cover the tech one first, because the law -- okay, the law one first because it's already there. Okay. Quite small, but anyway. I think even within the same country, right, several laws require different consideration conditions in order to do this kind of interception, the intrusive surveillance.

For example, like, our colleagues, right, are talking about, like, the requirement, right, before -- to get approval, right, to plant this software, what kind of consideration or conditions should be taken, right. For example, I try to compare our two existing law. On the left-hand side it's an app, on the right-hand side it's a special investigation app. You can see the difference, for example, one who can file a petition to the court, right, to get the court order or the warrant, right. For the computer crime act, any officers can file the petition, comparing to the special investigation act, that officer need to get approval first from within his own department, right, before contacting the court.

He has to get approval from the department chief first, right. And then when you see, like, which court that can approve this, can issue this warrant, in the computer crime act it's like any judge in a jurisdiction, right. But for the Special Investigation Act it should be the chief of the criminal court, for example. So you can see, even in one country, there is differences, right. And also, like time limits, or the measures that you should do after approval. You can see that in Computer Crime Act, there's almost nothing. But for the Special Investigation Act, it said in the law that when caught, going to consider whether to issue the warrant or not.

The court should consider about the rights to privacy, right. Or whether this measure is an efficient way to actually get the evidence, right. So if it is there and everything is ready, but there's no certainty that by planting the software into the device we are going to get the evidence that's required for the case, the court may not allow, right. Something like that. Also, there's a time limit, like how long this software can be there in the device, for example. So, that's one side. Maybe we need to think more about this in the context, not only about the communication, but also putting something into your device, because it's not going to be only the data related to the case that can be collected.

Once the software is planted in the device, any user behavior will be collected, whether it's related to the case or not. So that's why it's very far-reaching. So we need to think more carefully about that. Last part is the technology one. I think, like, more and more companies are trying to introduce a concept that help us more secure. I think two days ago, they just come up with a new model of the phone, right. And one of the features, it's about -- I think they call it memory scrambling, something like that. So basically, it's like at

the moment, a lot of malware are able to collect the data, because a particular app tend to use a particular area of our memory, right.

So maybe, for example, if our RAM, right, in our devices, the memory on our devices maybe organizes from the top to the bottom, some of the app may most of the time only use the memory at the bottom part, for example. So the malware knows if they want to get data from this app, they should look around this area. What they're trying to do is, they're trying to randomly assign the area of the memory to different apps. So each time the app has been used, it's not predictable, for example.

The thing is that it is very expensive at the moment. How to actually make sure that there is some -- okay, this will be our level to every device. Also, the fact that a lot of times these can be fixed. The patch is there. But the manufacturer feels like once they sell you the device, there's no longer a responsibility for them to update the software for you, right. So once you buy the device, it's like, okay, how to actually have some kind of law, like consumer law, for example, requiring the manufacturer to update your phone, I don't know, at least for two or three years, whatever. I think that's the thing that we have to discuss. Thanks.

>> K.S. PARK: Thank you. The last point is important for us, too, because we haven't updated our detection software yet. Prasanth, are you there? Prasanth?

>> PRASANTH SUGATHAN: Yeah.

>> K.S. PARK: Okay. You have your two minutes. Go.

>> PRASANTH SUGATHAN: Can I have my fifth slide up? Okay. So, while that is set up, let me get on with it.

>> K.S. PARK: The fifth slide? Fifth?

>> PRASANTH SUGATHAN: Yes.

>> K.S. PARK: Okay. Fifth.

>> PRASANTH SUGATHAN: Slide number 5.

>> K.S. PARK: Two minutes.

>> PRASANTH SUGATHAN: So, when the Snowden revelations happened, the one major discussion that we had in civil society was on mass surveillance, targeted surveillance. When we came up with the necessary and proportionate principles and how we should go ahead trying to tackle the surveillance. But now, this intrusive technology is more in the range of targeted surveillance. It is mass also, but more a case of targeted surveillance. The question is what kind of safeguards can we have. The slide you have currently talks about how telephone tapping or internet monitoring happens in India.

The safeguard that was introduced in the law -- after the Supreme Court direction -- was to make sure that the approval happens at the highest, at the secretary level. But we file the allegation under the Right for Information Act, and got information that on a monthly basis, 7,000 to 9,000 telephone tapping orders are passed. Can there

be any application, by a person of the highest level, who is going to approve 9,000 orders? What is the safeguard? Can we not have any judicial oversight? And so these are the things that we need to take into consideration.

Again, the proportionate principle that we all work together can give advice as to how we could have some sort of safeguards in place in the case of intrusive technologies, also. And then, of course, we need to deal with technology, how there should not be any backdoors, how there should not be any flaws in software, and how we should all work together. Thank you.

>> K.S. PARK: Thank you. Gul, you have your two minutes.

>> GUL BUKHARI: Thank you, thank you. A gentleman here said that domestic law might not be useful because governments share the information. If U.S. government law says you can't surveil your own citizens, they get the UK or Germany to do it and exchange information. So I think that is -- in my view, not correct. Because you can also then have legislation that my government will not exchange information with other governments. Having said that, there is a difference between mass and targeted surveillance. Normally one is aware that the governments are exchanging mass surveillance data, right, not very targeted.

Usually the targeted one -- normally, my government would be interested in the dissidents, the journalists, the NGOs, the HR activists. The U.S. is not going to give that to you. Domestic legislation is extremely important, number 1. Number 2, as everybody here as said, it needs oversight, not just judicial oversight, but from systematically, periodically, parliamentary oversight. There has to be a committee. They have to review, okay, so in the last six months you got this permission, so many applications. You have to demonstrate what you found from it, how it was useful, and how it was necessary and proportionate, even as a later check.

Very quickly, I think the domestic law must be every -- you know, like the question here was, what do we do now. What we all do now is given the fact that this intrusive surveillance is a fact of life, yes, we can -- by the way, by its very definition, isn't it not necessary and not proportionate, because you collect so much by doing this? You're obviously finding out if I am shopping for something. So how is that necessary and proportionate? So by definition, this technology is not necessary and proportionate, number 1.

However, when we lobby for domestic law or if it to be changed or amended -- I don't have enough time. But it applies human rights framework to communications surveillance. And there are 13 absolutely important principles that it lays out, which every domestic cybercrime law should comply with. I'll just talk about one or two for example here very quickly. You know, advanced user notification. We can have a long conversation, but you can look it

up later. The point is, the Pakistan law which we are drafting right now which is being debated in the Senate as we speak actually bans the service providers from giving advanced user notifications.

It goes exactly against the 13 principles. Then there is due process as one of the points in the 13 principles. And due process, very, very quickly, reads except in cases of emergency where there is imminent risk of danger to human life. In such instances, retroactive authorization must be sought within a reasonably practicable time period, which means without judicial warrant, right? Mere risk of flight or destruction of evidence shall never be considered a sufficient enough reason to justify a retroactive authorization.

Now, Pakistani cybercrime bill does exactly that. It says you can seize data or do arresting data without a warrant if there is a risk of night or destruction of data. And then it actually says the opposite. There has been no reference to these principles. So that is, I think, the most important thing. Yeah. I think there is a lot more, but basically, if we all, kind of, make that our guiding principle, it can take the teeth out of the surveillance. By the way, one other very important thing. The law being drafted is also section 36 -- six, I think -- refers to realtime surveillance. So realtime could technically include these technologies, not just tapping your phone. It could include this. So they're trying -- this and that, and this.

>> K.S. PARK: Thank you. We are out of time, but yesterday I remember that they had a lot of food at lunch. So you'll not run out. So, any question or comment? We'll just do five more minutes for question and answers. Yes.

>> AUDIENCE: Yes. I think you were speaking of two different things at some point. One thing is surveillance. The other is using technology, the context of a criminal investigation. I think the rules are different, and the legal framework is very different. So I think it's important to make a difference between those two scenarios.

>> K.S. PARK: Any other question, comment? We'll take more questions. Okay. Who wants to respond to the question that was just posed? Okay.

>> GUL BUKHARI: I think you're absolutely right. And our problem right now is that the law that, for example, Pakistan is coming up with actually mixes the two up, right. And they're calling it prevention of electronic crime bill. And it actually does not target actual crime, like -- okay. So we've been in consultations. The first draft, for example, did not even talk about pedophilia, identity theft. You know, these are crimes against natural persons. So now they've put everything into it, yeah. So it's investigation as well as surveillance, as well as citizens and natural persons.

So it's very, very -- yeah.

>> K.S. PARK: Thank you. I mean, it seems that the question posed was whether surveillance, technology would be allowed. And it seems that several panelists have said, yes, there are situations where it can be permitted, but should be permitted under stringent circumstances. And one of the requirements that the panelists mentioned was that the security of the user's device should not be compromised. But I don't know. I'm not a hacker. I'm not a techie. I don't know, when somebody hacks your one, whether that phone's security can be restored to the pre-surveillance stage.

I don't know if that's ever possible. So, if there is no question or comment, we'll end here. Thank you for your attention. Last one. Okay. All right. Yes.

>> The home secretary pushed for the bill to enable, like, the internet service provider can pretend -- and give extra powers for their law enforcement to do such intrusive surveillance. So could you foresee such kind of a bill will also apply, or some other countries will try to apply this kind of legal framework to do such surveillance work in the future?

>> K.S. PARK: Anyone? Well, the gentleman from Australia said Australia already passed a bill like that. And Arthit talked about the Thailand law that can be interpreted, or may not be interpreted to allow intrusive surveillance. So, I don't know about other countries.

>> CHESTER SOONG: Well, you are talking about a country that has already been monitoring 100% of internet traffic.

(Laughter)

>> CHESTER SOONG: Yes. You know, that's part of the project that was going on. I think the name was the Big Internet, or the big something that the UK government is operating which captures, I think, part of the crucial data they would keep for seven days, or a month, depending on the data. But the point, I guess -- and like I was saying, when the PATRIOT Act was enacted -- signed into law -- after the 9/11 attack, the answer to your question surveilling, we keep seeing terror or terrorist attacks at a large scale to any country, we might be seeing this kind of law being passed more and more, just because the citizens, they kind of feel threatened.

And they would tend to say, okay, I'll compromise on my privacy and I'll allow the state to do more surveillance. And hopefully that will give me a bit more protection. But as I said earlier, personally, I'm not objecting the state to do what it can to protect the citizens, which is their primary responsibility, especially the home department. The thing is though, the process itself must be, you know, must be justified and with an extremely good, clear oversight that's not simply by a court. I mean, the visa has a court to oversight it, but it wasn't very trustworthy, at least to the regular people. You

know. So, it's really how the whole system is set up. So, yeah, that's mine.

>> K.S. PARK: Okay. Thank you, we'll end here.

(Applause)

(Session concluded at 12:42 p.m.)

***

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

***