FINISHED FILE

ASIA PACIFIC REGION INTERNET GOVERNANCE FORUM
TAIPEI 2016
A NEW INTERNET ERA
29 JULY 2016
ROOM 401
1400 P.M.
WORKSHOP 19
CYBER SECURITY AND THE INTERNET OF THINGS:
IS PRIVACY DEAD?

Services Provided By:
Caption First, Inc.
P.O Box 3066
Monument, CO 80132
1-877-825-5234
+001-719-481-9835
Www.Captionfirst.com

***

***

>> MOHIT SARASWAT: Hello everyone. Sorry we are running a little late. We are waiting for some of the members that we had in other meetings. We are just finishing and we will start in another five minutes.

Good afternoon. So we are ready to start our panel discussion. I know it is a little difficult to have it after the delicious lunch, to have this panel discussion and still keep you awake. But I hope you will be -- it will be interesting enough. And I think this is a topic which is of great interest to all of us. Give me a second.

So the topic of our panel discussion today is Cybersecurity and Internet of Things: Is Privacy Dead? So we'll be -- I'll probably start the panel discussion with a quote from Eric Smith, the Google Chairman which he spoke during the panel in the World Economic Forum. The Internet will disappear. There will be so many IP addresses, so many devices, sensors, things that you are wearing, things that you are interacting with that you won't even sense it. It will be part of your presence all the time. Imagine you walk in to a room and the room is dynamic and with your permission and all of that you are interacting with the things going on in the room. That will be the impact of Internet of Things. I don't know what all things which we

are wearing on our body will be interacting with Internet. So your watch will be interacting. Your shoes will be interacting. Your clothes will be interacting. Obviously your mobile phone is interacting with the Internet. That's the power of the Internet of Things. There is clouds around Internet of things and what are the security threats involved when it comes to the Internet of Things. We will be discussing today during our panel discussion with our distinct panel members from various industry sectors what does the Internet of Things mean for them. Maybe for some of us it means home automation system. For some of us it means manufacturing system. For some of us it means medical equipment that are connecting to the Internet. We will probably try to explore during our panel discussion is there any common ground that we can come upon and define what it means for us, what it means for the Internet of Things. What are the unique intersecurity challenges that IoT brings on the platform. What are the unique perceived benefits from bringing increased Internet connectivity of the end user devices. Is it really a choice available to all of us. What could be the motivation in compromising the security portion of such IoT devices. And what could be the probable solution.

So I mean I'll give probably the panel in a sequence five to seven minutes to share their initial thoughts on this and then probably we will break down for a question-and-answer session. We want to actually have a very informal discussion on this because I think you are -- you are the focus of this whole discussion. Because you are the ones who are going to get impacted. So I would probably like to encourage you to ask all the intriguing questions you have of the panel members. So yeah, we have five to seven minutes for each of the panel members to probably talk about this. And after that we will have closure remarks and we will talk about privacy.

So I mean is there something called real privacy when we are talking about so many things connected on to the Internet? All our personal data is available on the Internet, shared with the -- in commercials, commercial organisation and everything. So I mean is there something called real privacy? So we will talk about that interesting thing during the closing remarks.

So I'll probably give a brief introduction to the panel members because I don't want to go in to details because we have such an amazing panel here. And if I probably go in to details we have to wait until the lunch. I mean until the dinner. So let's not do that.

On my extreme left we have Jon Lawrence. We actually lost oddly from APNIC who is the information security consultant but Jon Lawrence is a good buy I mean in place of Adley, is an executive officer from the Electronic Frontier Australia. Then to his right we have professor Peng Hwa Ang. As you know he is a professor with NUS Singapore. And then we have Shreedeep Rayamajhi. He is a blogger, social activist and also a steering committee member of the Dynamic

Coalition of Internet rights. It will be interesting to hear his thoughts from a youth perspective.

Then you are going to challenge me who is sitting in the center? He is a prominent information security consultant. Chester Soong. He is consulting a -- he is consulting Hong Kong Government on the information security system. He will probably shed some light on how the Government received threats from IoT. And then we have Zakir Syed currently with the SAMENA Council Pakistan. And then we have Satish Babu. He is a prominent free software activist, founding director of IC FOS and founding Chair of the ISOC chapter. I'll probably start with Jon.

>> JON LAWRENCE: Okay. Thank you. So as Mohit mentioned I was a little bit of a late bring in. I am not going to speak for terribly long, but I guess there is sort of a few high level issues that the Internet of Things rises. And clearly I am from civil rights, digital rights advocacy position. So the concerns around privacy and surveillance are pretty top of mind for me. I think -- I think personally that there are, you know, we are sort of in many ways already within an Internet of Things context. I haven't seen too many people wearing devices. Yep.

Okay. Good. So we have got, you know, fitness devices. We have got, you know, connected watches, wearables with cars that are talking to the Internet. We have got, you know, smart fridges and smart TVs. A lot of the issues need to be worked through and hopefully we can cover a lot of them today.

From my personal perspective I think the use case for a lot of these devices is really yet to be proven. I haven't worn a watch since I was about 12 years old. I never felt the need. I can probably see five types of devices where I am. You will never see me purchasing an Internet connected watch at any time. And I think, you know, many of these things, as I said there is yet to be really proven a use case and a demand for them. And the Apple watch hasn't exactly taken over the world. We will see how that goes. And it may be me being a slight model lite. That's I guess in terms of consumer devices.

There is a whole other range of industrial where there is a much more obvious and compelling use case. I think in terms of things like wearables and other devices and we kind of already there, much of what I am going to say already applies to the Smartphone in your pocket. But, you know, we are sort of getting to a point where we are going to have completely pervasive and comprehensive surveillance in everything you do in your life, potentially including every beat of your heart. And that to me is a pretty, pretty concerning situation. And I think there is a genuine kind of possibility that we may actually sort of start to lose some of our humanity in all of these technologies. That's a general personal concern that I have got.

I'm sure that we will go through all the security concerns and so forth. The amount of data that's going to be generated by these

devices, of course, is just astronomical. We need to be careful that we are not overcollecting that. We need to sort of be ensuring that we are, you know, dealing with concepts of data minimization or data austerity and spasm kite which I quite like. And we need to make sure that we are using open standards so that, you know, everything can talk to each other. And particularly I think we need to make sure that we have opportunities for people that don't wish to use these sorts of devices to, you know -- so that -- I mean I am fairly certain you can't buy a car today, a new car on the market today that isn't somehow Internet enabled. And as long as you have an opportunity to turn that off properly and opt out that gives me a certain degree of comfort. And with everything privacy related it is about you having an ability to make a choice to be involved or not. That's a very important point. So I will leave it there.

>> MOHIT SARASWAT: (Off microphone). Giving choice to the consumer. So I mean probably educating them, making them aware of what are the risks associated and leaving the decision to them and you raise an important point that it might not be a choice going forward. I move it to Professor Peng Hwa Ang.

>> PENG HWA ANG: Hello. Good afternoon. Let me begin by making things more complicated. There is personal data protection. There is privacy and then there is information and they are quite separate. Let me show you how they are separate. You think of personal data, you think of personally identifiable data. Your name, phone number, passport number, credit card numbers. Personally identifiable data saying you are who you are. This is different from the privacy which can be your secrets to health, maybe do with money or more commonly the lack thereof. Your drug habit or vitamin habit. The mistress if you are old enough, porno if you are young enough. The whole plethora of things about you but doesn't necessarily identify you without knowing your personal data. You need the match of personal data and secrets. And that's how you get a validation of privacy. There is one more area that's kind of interesting for us. I have this fitness tracker. Very cheap. Less than $20 including habit monitor. This -- the version that I had before I installed, you know, an alternative software app, the version I had actually wanted contact details of all my friends. If you happen to be on my list -- here is what 9,000 contacts here or some duplicate. You would be -- you would possibly have my -- the contacts being sent to somewhere in China without knowing it. This is really a personally identifiable data because I would have your name, probably a phone number, your address, your working place, your occupation and so forth. And your privacy would have been breached without you knowing it. Fortunately the guy who reads fine print, the privacy, because I teach the class, I didn't install the app. The version they have now they say they respect privacy but what do they mean. I install another app and it takes all these contact details. So this is where it gets risky

because what you have now although you may protect your own privacy you are very careful, but someone that's out there may not be reading or may not be aware that these details are being taken, this person could breach your privacy without you knowing it. This is a pretty scarey part about the world we live in now because of the prevalence of the -- or rather the ease with such data can be taken. I have done a bit of a study looking at apps and the notices that report. And in Singapore I estimate about animation, about half, more than half of the apps actually breach data protection laws in Singapore. Meaning that in most cases they overcollect information. So this is independent even of your IoT which may or may not breach privacy depending. Because apps are on your phone, on your laptop and so they identify you. Because typically you are the one using your phone, using your laptop. So they can track it down to that machine or that phone that is really about you. So what it means is that the title is whether privacy is dead. Privacy or data protection should not be dead. It should be even more alive. It should be even more alive to protect us so that companies who put together do not overcollect the information. Why do you -- because all my friends, all they need to know the fitness of me. Why do they need to know the phone numbers of my friends? If they have some privacy laws, data protection laws then they must be able and willing to enforce those laws. So to the extent, therefore, I would say that IoT because even greater awareness of privacy and data protection laws and enforcement of such laws. Thank you.

>> MOHIT SARASWAT: I think you raised a very important point, it is also not only the users I mean but also I mean there is a responsibility with the intermediaries and other parties which also have to provide their collecting data. Thank you for that.

Now let's move on to Shreedeep Rayamajhi. I would like to hear from you. What does youth look at from an IoT? Are they looking at IoT as the next thing? Are they aware of the risks associated with it? What are they doing about it?

>> SHREEDEEP RAYAMAJHI: You know, especially when you look at it from the youth's perspective, you know, it is like technology rocks, right? It simply rocks. Like you have these devices that are like so fascinating and fast and good. And you can do so much stuff. So we are more thinking about let's give it a shot but as Peng Hwa Ang said we need to focus more on the safer side of it as well. When you talk about technology, I strongly believe that technology is like a knife. It is about how you use it. So it is all about the morals and values and the things about it. And especially if you look at the South Asian perspective or the Asian perspective, then it is something like a technology has been transferred to us without, you know, without any preparation. We are like -- we just got technology. We are just evolving in most of the countries in Asia. So there is a basic need about developing the core values. About, you know,

technology Human Rights, cybersecurity, all those things and we need to work on it. And we have not been working on it. Like on real terms if you look at the cybersecurity policies of Southeast Asia, you know, they have a standard. They are all like up. But when it comes to practice, things don't work out. We have freedom of expression, but do we have it in reality? No. That's the real case. And why is it happening? It is because we are not working towards the core values. We are not developing. We are not targeting. Like we have core studies which focus specifically on what is computers. We need to have sessions. We need to do some capacity building, raise awareness in terms of political leadership as well as youth. So that's like something where we have to work.

>> MOHIT SARASWAT: Thank you. I appreciate your reactions, particularly from a youth perspective. And I also like your energy. So let's move on to Chester. I would like to hear from you particularly on this issue. What information security has to say about this issue. And also how does Government look at it. Are they doing a proper risk evaluation when they are going to probably connecting our energy and utility sector because that's one of the things that they are considering in the subcontinent. They are considering more and more I mean automation when it comes to your utility sectors and which are key areas and which might be having a lot of impact if you don't do a proper risk assessment.

>> CHESTER SOONG: Well, to me I guess the security and privacy of IoTs comes in I guess two aspects. First, of course, the security which is I guess the protection on data, you know, on devices. And second is probably the information that it collects, like the breadth and depth of this device because it goes like -- because we were saying it goes way in to your health information, your car, your habits. How much -- just you are using on a daily basis which is quite intrusive. What you like. And now I guess on the security front there are many people I guess both from industry and academias on cryptography helping to provide securing the data inside. Now but my concern on that is, you know, we all know in a security profession, I mean the IT security professional that things change too fast. I mean, you know, I don't know how many times you have updated or, you know, upgraded your software, your mobile phone or apps, softwares on your computers in the last three months, you know, and not to mention the box and security that we mentioned on systems. And it is -- this has been happening to audio devices. And in some other security conferences, hack conferences people have already demonstrated hacking in to cars. I mean, you know, and remotely controlling it. So this is not like the future. This is today. And I guess my experience not only advertising Government but also working at DPA I think this -- it comes in a breath where I guess good Government, a lot of them are not ready or they don't know enough, basically to know how to protect the personal data or the privacy of -- on these

devices because, you know, a lot of it, first of all, we need to know what is personal data. I mean Professor Peng Hwa Ang mentioned something, a concept that we need -- we all need to know which is personal data, privacy and personal privacy. A lot of times when we go to privacy conferences regulators talk about personal data privacy. Not your personal privacy. People they confuse the two. They thought okay, regulators should protect if they are looking after privacy. They are looking after your personal data. And that's -- and what our personal data they have -- they are defined under their respective laws.

So what you -- for those, you know, data or metadata that are collected by the device, by the audio devices a lot of them are not defined under their respective law. So that means they are not protected. Unless, of course, they are sampled together, you know -- we say that but I think sadly to say sometimes this is used I think by DPAs not to do further action because if you -- when we think about further steps to enhance this picture we have to go back to legislation. And that's a big barrier. You know, the head of DPAs they are often reluctant to go to that step which is quite -- could be quite challenging to them. And I think one I guess last comment I'd like to make is to your questions, I guess you mentioned like the question is whether privacy is dead. The world is changing. That we used to -- privacy used to be -- used to mean your secret or secret or things that you like to keep to yourself. Not necessarily, you know, super sensitive or embarrassing but something that you don't -- you don't necessarily want the public to know. But today, you know, with the help of the Internet and especially mobile apps, IoT devices, it becomes, you know, an area or a space that is heavily controlled, monitored, and, you know, and is full of actors, players who are like even trading of this information. So I think it is just that the rule of privacy is not the same as what do we expect or we knew.

>> MOHIT SARASWAT: Thank you. The rules are changing. The privacy rules are changing and the definition of security to some extent is changing. And you made a fair distinction when it comes to what is personal privacy and what is the privacy of personal data. That's a fair distinction you made.

Now we move on to Zakir. We would like to know Telecom sector being a core part of this whole transition from being connected to the Internet to machines connected to the Internet. There will be a lot of machine-to-machine talk happening and Telecom sector will have a great role to play when it comes to secure data transfer also between machine-to-machine. So is the Telecom sector ready for this transition?

>> ZAKIR SYED: Thank you. Telecommunication industry, the overall access technologies or ecosystem is so very important to the debate. At the end of the day the telecommunication system and ISPs

that enables us and you the IoT providers, service providers to be able to access data, to move it within the borders or crossing international borders which is a cause of concern for a lot of segments within the industry. So you see Internet, this Professor Bishop Howard said you don't really know exactly when the transition will take place. The idea is that you have to understand it and then get prepared for it. So the actual thing is that we need to be prepared for it. IoT in itself is sort of a disruptive technology from -- from its application's point of view. Have very good use in health, in automobile industry and agriculture and education and realistic -- every sector we got a very good use of IoT. But the problem arrives when it plays with your privacy. Not privacy or monitoring. For example, I don't have problems with my data being monitored or surveyed or compromised or whatever. I have a problem when the decision is based on that data and that is the problem with big data. When big data is combined with IoT and infringing in certain algorithms and then being used by different entities to be able to arrive at a conclusion and that is something that is dangerous. And I mean that -- for that I mean the industry, the different stakeholders need to convey and come up with something real, really, really, you know, practical in terms of privacy and stuff like that.

Coming to your point about telecommunication, for example, you see -- in the industry we have been getting very interesting statistics. Gardner, for example, they are telling us there is almost 7 billion devices connected to the Internet. Cisco and others claim there is already 17 billion devices connected to the Internet. Yeah, actually the industry, the IoT industry is evolving. It might be slow in South Asia. Might be fast in Pacific or Europe. It might be, you know, at a medium speed in the Middle East, but the fact is that this is something that really is coming in. And we need to be prepared for it. So in terms of the telecommunications and the excellent industry they are not prepared for it. The reason behind in the previous version we were discussing it on the technology front we are evolving. There is a huge amount of investments and innovations that are taking place in industry, but on the policy, the regulation and the legislation and I mean that is something that really needs a huge amount of work to be able to face this, you know, this IoT thing which I personally call it -- I don't call it Internet of Things. I call it weapon of mass destruction. Because it is creating, you know, disruptions in every aspect of our life, every aspect of our life. So I mean it is very innovative, very disruptive technology. The fact is that we really need to build capacities and share experiences and to be able to be ready for what exactly is this going to be in the future, in the near future. Thank you.

>> MOHIT SARASWAT: Thank you. I thank you for your comments and your thoughts on this whole topic. But I just want to highlight one point which you made data by itself is not disruptive. But what

is disruptive or what is dangerous is when organisations, Governments start making decisions based on the data. I mean which is very personal to you so far in the sense if there is an example of an insurance company which just hikes your premium because you are probably driving at a very fast speed or probably you are not a very safe driver or maybe something else here.

>> ZAKIR SYED: This privacy thing, for example, I am using an IoT application or a Smartphone application and because of my being -- using an IoT application somebody else's privacy is being compromised. My device might contain my contacts and pictures and stuff like that when that data gets to the server of the IoT service provider. So there is something, you know, somebody who is not even using that IoT application, and then his -- and his or her data is at the same time being compromised and it goes to there. That is something that again the decision that is being made on the IoTs and then again the privacy of others who are not actually using IoT applications, their data or their privacy is being compromised. So that is something of great concern.

>> MOHIT SARASWAT: Okay. Thank you. If we have Jahangir on the line. Okay. To our rescue we have Satish. Whenever we have an issue we are always going to technologists. We have heard solutions when it comes from law enforcement, from regulatory perspective from both Peng Hwa Ang as well as from Chester. This could be a problem solution. Now probably we will look forward to technological solutions, what could be the I mean solutions which the industry has to offer, to probably mitigate these threats which are coming along.

>> SATISH BABU: Thank you and very happy to be here for the session. The theme of our regional IGF is Cyber Physical World and So On. And IoT has a very prominent place there. And when you integrate we are having the grand unification which has got only kind of impact coming up. The first problem that I see is a problem of the dump user. All of us have been dump users at some point in our lives. The problem is that there is a one billion dump users joining. Now when you put this one billion with the fact that some of them may be careless in using the Internet, we have a huge threat that comes up, the threat vector of this one billion people. Not all of them are going to use IoT devices directly but the mobile phones is also now an IoT device. So from that perspective this is a big risk that is going to happen. And when you note that this one billion is generally people who are not so educated, not so well off, the threat becomes magnified. That's the first point.

The second point is that already so many human comments. Internet of inaffected things, Internet of insecure things. People are predicting all kinds of things on to this IoT, basically the risk kind of project. And also we have things like implantable and ingestible that you can swallow. And these are operating very close to my body. I mean, you know, I have a right to know if these things

have any security angle to this. So these are new issues that are coming up which are perhaps not there in earlier generations of data. And this insurance company thing that was mentioned right now it is a big problem because the moment the data becomes kind of public, it can be kind of leveraged by business entities. We have smart cities. Smart city, what does it mean to hack a smart city? Today you cannot hack a city but tomorrow you can hack a city. A small grid.

India lost power for 5 million people some time back but that's because of cascade dripping of power grid. We have not defined the problem as of yet. So the magnitude and the scale and impact is not known of some of these things. Citizens, I was reading a thing where they were saying smart city, citizens are city sensors. Whether they like it or not you install an app and you become a sensor and people start reading things through you. We don't know whether it is being used that way. And we have also this IoT. Many of these devices are arrays of a single device. You hack one you hack all. So it is very easy to get in to scale. There is no human intervention.

So my point here is that when there is no human intervention, missions are deciding on our behalf, I pointed out in the first session, and issue of autonomous car is going to hit something. Whose life should they protect? The person sitting in the car or the person outside and who decides this. The software is going to decide this. Who should be deciding? On what basis should society say that somebody should be deciding on this. Liven that issue. These are issues that come up. And as an open source person I strongly feel that some of these things should be exposed and the code should be exposed. And as a programmer my currency is code and I deal with code. You show me code I'm happy. But if you have an obscure code device that is sitting close to my heart and nobody knows what the code is then I have a problem with that. Thank you.

>> MOHIT SARASWAT: Thank you, Satish. I mean you highlighted some of the key risks associated with the technology. And what you brought forward there is not much of awareness. When it comes to what are the threats, I mean which this can probably pose to the whole human society and further -- I mean community. This is one of the prominentities and why there is not sufficient debate of the security risk associated with it because when it comes to more security breaches like when it comes to financial fraud there is a huge tangible I mean -- we can actually quantify the break, but when it comes to these kind of IoT kind of breach we don't know. I mean what if somebody reads my data from my page. I don't know what are the security threats associated. So I mean that's great to hear from the panel how we will probably open up the I mean Forum to the questions from the -- yeah.

>> I was -- ICANN is registered in California. As you know the senior officer in California by law you have to learn to our causes about sexual harassment, to our (inaudible). This is by law. So leads back to the IoT. If the IoT, because IoT is designed by engineer,

but the problem is that many engineers they don't have legal background. Okay? But in many of Asian countries we already have data protection law. I think in Taiwan, Singapore, Hong Kong, many already have that.

I think we should acknowledge the Government as in IoT company, the engineer, at least they need to understand the data protection law. Because they don't have a legal background. They don't know what the product they develop. The legal, the data protection law.

Second when IoT design as we know this is a certain Internet pool. In most of the cases many of the engineers never really cared to shut off those support, is not necessary. So we should have to ask an engineer they have to limit the ports available. So limited information. For example, in Taiwan as you know many years it is underdeveloped, even now. We find most of the APP development, they leave all the ports open. It is crazy. If you -- leave ports open, how you can tell me they are secure.

So let -- at least something that we can do. Give the engineer a legal education. Give the engineer -- they should not open all the ports unless it is necessary.

>> MOHIT SARASWAT: Sorry. Do I want to answer that? One more question, Mr. Satish. Sometime it is a hardware problem. You can't patch a hardware problem. It is an increasing problem because Internet of Things is not just a software thing any more. Everything is not Linux computer. Something just achievement hardware bringing together. Right.

>> CHESTER SOONG: Last thing first I sort of -- I respectfully disagree with this hardware software, because there is no pure hardware or hardware contained, but I certainly understand where it comes from. The problem with a lot of these devices they cannot be fixed by the end user, by the owner. The owner has no access to what's inside. Not even the configuration. You have a car, you know, most people don't know how many computers are in their car, not even -- what they have right now. And that leads to an issue that I think is important from the perspective on how IoT devices are getting so popular or fast growing because of this cost, of this low cost. And you can imagine like with a sensor that's -- that costs you less than $1, you know, like I think it is what, 12 cents or something. I forgot the current price what costs for that. But how much you can from that percentage, how much you can really put in on assuring the security of that device sensor is up to date. And first like I said, you know, we have a lot of people working on securing the information on the devices or sensors. But what you -- but what happens after they are shipped outside the factory? Do we have cost? Do we have the resources to make sure, you know, those devices maintain, secure, you know, six months from production, three years from production, from, you know, sale, right? And so I guess feedback to the question or comment is something that I kind of thought about before, how can we improve this because from a DPA's perspective it is quite impossible

for the DPA to have the authority which I wish they had but the authority to like examine and review, you know, all these, you know, the applications, use of these audio devices because they are crossing so many expert -- aspects of someone's life. And so broad from so many industries.

So from Government's bureaucratic structure it is hard to have one authority to look after that and this is one of the few areas or applications that I would actually prefer the protection of personal data or privacy in this -- in this concept of principle of protection rather than the Human Rights.

>> MOHIT SARASWAT: I think you raised an important paradox we have in the industry where the whole intention of going to IoT is cost savings and we bring on top of security. Industry has to kind of digest this, that it is no more an overhead but an integral part of this. So we are talking more security with design. Security by design.

>> Yeah. Sure. I was going to add to that as well. That yes, the point noted that engineer's legal training and so they may not be aware of what they are doing. But that's not really an excuse for any product because you -- product out there it has to be safe for the consumer and has to be safe to meet your standards, comfort. So I don't see why in the case of your IoT that it should be any exemption at all. It should just meet your safety norms which in this case happens to include possible data protection. And I don't think it is really that complicated. There should be some kind of understanding that you don't overcollect data because actually you are exposing the liability. The more you collect the more you must keep secure and the more you must prevent leakages and that increases your liability. So I think that some basic understanding should be necessary in when you have this IoT, especially if you run your product with a major consequence, like some major impact worldwide. If you want it to be small that's okay. If you want to be big you have to play a different game all together.

>> MOHIT SARASWAT: Do we have any other questions?

>> Yes. I would like to shift the discussion a little bit. I think one of the main issues with IoT is that we need to rethink how we come up with ideas and ideas around the data environment. And to give you a simple example is this smart city discussions at the moment and what you see all over the planet is that cities come up with the most boring suggestions which are completely based on public/private partnerships. And they come up with some traffic data collection and some optimization of utilities and so on. But what is missing and what's also more coming in to this course is that we need open innovation and open innovation means that we create models where the data objects or the citizens are actively involved in shaping the data environment. That applies to insurance companies. It applies to car companies. That means in everything where the human being is

also somebody who sends and collects data is involved in how we shape our environment. And I think that is really the biggest challenge that we have, go away from public/private partnerships to public/private people partnerships and that's happening, for instance, in Amsterdam. Here, for instance, an open sourced citizen IoT which is the themes network which is based on Lorawa. And this is very low cost IoT solution and I think it has triggered a lot of ideas coming from the citizens on how to make the city more liveable, more safe and more enjoyable without relying on the big IT solution providers. And I think that is actually what could come out of this whole IoT discussion and how to involve a needs based innovation discourse. Thanks.

>> Sure.

>> SHREEDEEP RAYAMAJHI: Okay. So actually -- it is on my phone. I assembled the sensor within five minutes or so. By the way I don't want to expose the API. So I don't want people to know that nobody is in the office. But it already happened. It is actually Internet collected devices are already one of the hot topics among hobby electronics. So I think it should check to make it further. Thanks.

>> When I can retrieve, we actually face it one of our IoT companies. The company ideas are marvellous. The company don't control the data. Consumer control your data and I think that's a good design. Now IoT design from them they don't collect data until consumer agree. So thinking about it we should educate the people that is like design.

>> SATISH BABU: A couple of responses. I completely agree with the whole innovation at the grassroots concept with the five dollars and several other quotes now. It is possible to have grassroots innovation happening. I was same cities doing sensible things with whole IoT concept. At Los Angeles a year back the IT head of the city was talking to us. This is an ICANN meeting and he was saying we have used IoT to convert the written policy of the city to actual practice. The written policy was public transport shall get the highest priority in all kinds of traffic. We were asking how has IoT helped in this. So he asks the question back, how do you think you can get the fastest from one end of LA to the other end. We said you get a fast car or motor bike. He said no. Follow the red bus. It is public transport. They are so wired with sensors. Whenever a public bus goes it becomes green. That's the fastest way to get across the city. This is what the policy says that public transport gets transparency. That is a very insightful thing for us because we felt this is a good use. We are a viable city like this. So the smart city is still unfolding. I do not know how creatively people will use this. The whole data ownership and bunch of risks are there. But I think there are also both level the grassroots innovation as well as some cities which are looking at it out of the box. There are possibilities.

>> I like the idea of having securities by design. Think about

the security aspect of the device. For example, if somebody used that device in the future what kind of security tips will be there. So that kind of thinking should be there from the beginning. And if they think that there will be such securities in future, when people are using these devices, there should be a mechanism to update the device. For example, if they think there will be problems in the firmware or the operating system of the device, there should be a mechanism to update the device remotely by connecting to the Windows server, et cetera. This is my comment.

>> JON LAWRENCE: Thinking as a nontechnician one of the biggest challenges is keeping things updated and particularly when you are dealing with manufacturers that are not sort of from the technology space originally I think that's a massive challenge and one I guess sort of questions that comes to my mind what is the potential for, you know, 10, 15 billion kind of not terribly updated and patched IoT devices being sort of harvested in to a massive server Botnet. That strikes me as a pretty significant risk.

>> Yeah.

>> SATISH BABU: I think this issue of Botnets Vint Cerf is known for talking about this thing. Example of what this kind of thing can generate in to. There are actually protocols that have evolved to update on the fly these devices but there are severe constraints. They all use very low power stacks. So the stack is severely truncated and made low power. There is huge sensors on -- there is only one gateway and all the external kind of contact has to be through that gateway and this imposes structural constraints on how efficiently you can do this update. This is a risk.

>> MOHIT SARASWAT: You have a question?

>> Yeah.

>> MOHIT SARASWAT: Do we also have a question from the remote? Is there any question from the remote? Okay. Go ahead.

>> Hello. I have a question. It is sort of related to IoT, but assuming that we are surfing on the Web and we enter a website and a website doesn't request, store the user's permission to use cookies. So then as far as I know cookies actually are short-term memories for website. They actually trace whatever you search on a website and keep it as the data. So next time you visit they actually will know what you are going to search in your preferences. So I'm not sure from Asia but in Europe they have policies for actually asking for permission for users to either accept the use of cookies or not. But do you think that the lacking of the permission part is unlawful or should the part of either the user should be asked the question of yes or no using the cookies, is that a mandatory thing or is that -- should that be kept unaware of so then the user can just go on being unaware of actually their -- them being monitored and being collected as data?

>> ZAKIR SYED: Okay. Thank you for the question. Real

technical actually. Asking a user for, you know, accepting or not accepting the privacy -- the cookies policy, I mean if in a particular environment there is a law on it and application or web service provider they are not using the (inaudible) obviously is a violation of rights, a legal right. In the European Union we have a law on that and that's when you visit a European who has website. So you actually get this popup asking you for do you agree to the cookies policy or not. So if, for example, if you are accessing a website in Asia you don't actually get that popup. So that's why we cannot actually say that this is kind of, you know, illegal because we don't have a legislation from a regional body or, you know, an organisation that actually had enacted something to that -- bound the Web service providers within Asia to, you know, adhere to those principles or to those laws. So I mean in a region where there is no law and it is okay for web service providers to provide -- to not ask the user for the cookies thing and if there is a law and they are not using it then this is a violation.

>> CHESTER SOONG: What you are referring to is the cookie law from the EU which is kind of regarded by the data protection experts as failure. Because it kind of warns users before they visit the site, but they leave very little choice in terms of protecting because the other option you don't choose, you can choose is not to visit a site. I mean don't visit a site or you accept what they are planting in to your computer, on your browsers. So it is sort of like different -- not I believe the model is perfect but what, for example, current version of Android is doing, at least it shows a little bit of improvement on that front because if you -- if you install an app on your current -- on the Android device now, the current versions, basically, you know, the app has to apply or ask the user for permission for each of the app's privileges that the app has or you have the option to turn individually off after you install the application through the app. So I see a certain level of improvement on that, but, of course, how Google or how, you know, the various developer of the variants of Androids enforce that is something else. Yeah.

>> JON LAWRENCE: I think that sort of brings us nicely back sort of in the concept of sort of opting out and I think that kind of granular opt out is important particularly with some sort of consumer device. Just a binary on/off thing in most cases is probably not really very valuable. It is likely to render your device fairly depending on what it is, it may render it fairly useless and therefore essentially meaningless. Having that capability to, you know, really get granular control over what you do, perhaps I might have a Fitbit and I want to sync it with my iPhone but I don't want to sync it to the cloud that's entirely appropriate. Should be able to control that sort of thing.

And I think that's a really important part of sort of this data control and how we move forward. One example I wanted to throw out

there and I suspect this is happening elsewhere as well but we already have health insurance companies in Australia that are doing trials with customers sending them a Fitbit or equivalent device and sending them certain health challenges and saying if I can meet these parameters, such as 20,000 steps a week or whatever it is and certain other things, then, you know, we will give you a discount on your health insurance. Now that's all well and good. I imagine that's a fascinating experiment for them and they are generating some really, really interesting and valuable data. The problem is we sort of therefore are kind of heading to a situation where essentially anyone, potentially where anyone that refuses to use one of these devices in the future will have to pay a premium and that's a concern I have. There will be genuine financial, potentially also social costs to opting out of these things. And I think that's something we need to be weary of. And, of course, that already happens to some extent. There are social costs to not using Facebook that are very real. We need to make sure that the concept of opt out is real, is the point I am trying to make and that's not a straightforward thing to do any way.

>> MOHIT SARASWAT: Any other questions from the -- yeah.

>> Okay. So there are like a huge usage of IoT devices, like IoT cameras and gateways these days in households. However most people they don't know how to really set up these things. So they just use default settings or they just plug and play which is very dangerous for security reasons. You can easily use Google search to banner grab these devices that are not protected by passwords because they didn't do it on factory settings. So what you are seeing neither regulations that can do to enforce or to improve on the factory settings like forcing users to change their password on the first time or policies like these.

>> SATISH BABU: I think this goes back to my general point about dump users. All of us want to buy something and immediately get results. Default settings are a huge problem. Cameras are left open like this. So I think user awareness has to happen. As a generic cross-cutting thing because every single device it is going to happen. There was a generation back, 10, 15 years back there was a case of new systematic administrators buying up a Windows or Linux box and installing it. That had so many vulnerabilities. So the next billion that is joining with these kind of devices we can have some factory programming okay first time you change settings, but still people find out a way to get around that actually. So user awareness building is very key to this.

>> MOHIT SARASWAT: I think by the time the mic is coming -- I wanted to have a follow-up question on what the gentleman asks. When we talk about this cookie business I mean while we have some regulatory measures which kind of educates users about what they are getting in to. But don't you think it is just about transferring the risk?

I mean we are just making a user liable for his action. And I mean to be very frank though we are technologists. To some extent we all accept the cookies. It becomes a matter of using it or not using it. That brings me back to Jon's point. We should not -- I mean if -- there should be a choice available to the end user that if he really were to have that risk and still want to use the service. It should not be a denial of service for him if he doesn't want to probably have accepted the cookie policy. So probably some of the panel members can answer that. Yeah.

>> Okay. Thank you. My name is Rim. I live in Taiwan. When discussing things like that, I used to -- I like to think about the ecosystem problem because it is a very complex problem. So we can say that there is a technical problem. There is an economics problem, et cetera, but especially interested in two points. Just said that the Government is not ready. And when we talk about privacy we all -- many persons will think that the Government should do regulation, law enforcement, et cetera. However does that really make sense? I mean in the -- in another conference where we were talking about is surveillance justified. So perhaps Governments are those who want privacy to be dead? And especially for some Governments who would like to know more about their people. So they can stop crime. That is a question. Or they can attack their enemy in politics. And/or this is never the important thing for politicians. Things related to both are. Like building roads, building bridges later on that may be the money source of some politicians. So when you are interacting with Governments is things like this really something that Governments pay attention to?

Because if it is not, it will never be resolved. That's from the perspective of an ecosystem. And I will tell my second question together. And when Professor Ang mentioned that companies should collect informations just enough, just enough, but in the big data world where data is money and the company, there are a lot -- there are many companies that they haven't figured out a way to make use of the data. So they may just think let's collect it now as much as I can. And as when we are talking about liabilities, you just mentioned, but like the show me, you just show this, for a company like those in China, privacy is that really an issue or for those companies to their benefit they would like to collect as much data as possible as long as regarding liability perhaps that's never an issue. And I don't know. That's just my personal thought, but I'm thinking from the perspective of an ecosystem. Thank you.

>> I am not very ugly about it. I am responsible. The Government, the company if they want to collect the data, unless there is a data protection law, if they have a data protection law, they collect more data than the data protection law allows. They are already illegal. First in -- I don't want to convey -- we are talking about China because they don't have a data protection law. Okay?

But thinking about it if such Government is doing the same thing, in Europe, look how European, France, how the France find the Google harmony money, billions of dollars. A billion dollars. Unless your kind of company you don't want to survive. So no excuse to be honest. Unless the country they don't know. Such as in Taiwan where data protection law. If you collect the data, more than you need or illegally, sorry, you already violate. And just the chance for somebody to go to the court to show you. So I think any company have no excuse. So I don't know. The data protection law is published as in Taiwan, more than three years. So I believe in Singapore can you do that? Say I don't know. So I can do it. I don't believe it. What about Hong Kong? You have data protection law, right? My company, I violate data protection. Collect illegal data. Is Hong Kong Government agree? Say oh, it is okay. I can give you excuse. That is wrong -- that is -- no excuse law.

>> JON LAWRENCE: So I -- I certainly have no knowledge whatsoever of Singapore's data protection. In Australia our privacy laws set standards and principles but certainly doesn't in any way prescribe what information can and cannot be collected. And I think to go back to sort of your question about, you know, do Governments -- do Governments have an interest in this data and the answer is very obviously yes. I think we have seen -- we had a debate in Australia over the last couple of years, the way the legislation is worded would start to incorporate data from IoT devices potentially. And, you know, in the name of national security and, of course, watching, catching pedophiles is the other excuse. We have what I think is a fairly extreme retention policy. We have a two-year period to some extent still working out the details of what is being collected but it is clear that Governments would like the data to be there in order that they can go back and look at it just in case. And I think if you think about the sort of data that's already been collected, so with your mobile phone that's, of course, including your location, whether you make or receive a call, make or receive a text. And if they get in to the cell data then even just the fact that your phone is on you can be tracked fairly accurately. That's an intrusive situation there which is tracking your movements. If you add in things like an Internet enabled car, if you have a smart house with an electronic device that opens your front door, that records that in a log somewhere, all this information will be of interest to law enforcement and intelligence. There is no doubt about that. And the question is, you know, is it appropriate for them to have access to that. One of the biggest challenges we have in Australia is all this data is available without a warrant and that's obviously considered at the moment, but there is no doubt that Government coming from the sort of law enforcement intelligence perspective they would like the data to be there in case they need to go back and look at it at some point. And I think the experience we have is they will ask for as much data

as they think they can get away with it. We need to fight them.

>> PENG HWA ANG: Yeah, I agree about the case that the gentleman mentioned that data can be collected in almost like a direct net kind of thing. The data protection laws generally speaking do not allow this. You cannot collect data just in case. You have to specify why you are collecting the data. You have to specify why this particular bit of data and it is kind of a common principle with all data protection laws. So let me give you one case where this -- I have a cell tracker and cell phone. My student ask you why body work phone. The cell phone when it first came to Singapore it violated the data protection law because it send contact details of phone back to China and whoever bought phone started receiving from China. It doesn't break the law in China. But it breaks the law in Singapore and they will be fined. They stopped doing that. I don't get Spam from China when I buy the cell phone. So I think it covers the point that even though you may be a company operating out of some jurisdiction in China which has no data protection laws. If you want to play the game globally you have to abide by global norms. This is what the world expects. If you don't want to play for global norm that's fine. Once you go global you have to adopt your best practice and global norms says you can't collect data just in case. And in talking big data, I often see companies collecting portable data but it is often called data exhaust.

Look at all of us here in this room. We are data exhaust not from positive body but from a mobile phone. And the data exhaust there is a mobile phone here. It is not moving. And once you move on the road then you can see this dot moving and I have seen some of these plots showing the plots on -- in traffic. And if, for example, you see the dots are not moving on highway details traffic jam there and that's how we use some of the -- how we use big data for some of this use. Big data doesn't necessarily break data protection laws because knowing that phone is there just phone doesn't say who it is. Just the phone is there. So big data can still survive and thrive without necessarily breaking data protection laws.

>> MOHIT SARASWAT: Thank you. In the view of time we won't be able to take much questions now. But I think I just want to have a last question to the panel because kind of insist on gender balance. Maybe it is not related. But I would like to ask is there any specific risk of which IoT kind of poses to specific gender or maybe specific demographics? Is there anything? I mean unfortunately we didn't have any panel member from other gender. So probably, yeah.

(Laughter).

>> MOHIT SARASWAT: Huh?

>> (Off microphone).

>> MOHIT SARASWAT: Yeah. I'll take that blame.

>> SATISH BABU: So here is interesting news that got reported. We are all aware that we use the car ride hailing applications like

Uber and Ola. And there was a case when a researcher was finding out what the app is collecting from the mobile phone and giving to the back end. It collects battery level, currently the signal level of the mobile phone and date and time and it is pushing it to the back end. The question was raised why is the back end record all of this. It so happens that these cars, I mean the systems have two prices, normal and search pricing and what is happening is if back end users, this person has low battery in a low network place if so charge him or her surge pricing. If you also know the gender of the user, you have a situation that late at night low battery, low signal is a woman we charge surge. Now this is a differential impact. I mean the company, of course, refused. The company said we are not doing anything of this sort. There is no way to kind of look at that. So it is actually a differential impact on women if such a thing is happening. Thank you.

>> MOHIT SARASWAT: I didn't expect an answer to that. Somebody want to add anything? We will move to the closing remarks. So I have specific questions now. I just wanted to ask from a panel that we always probably criticize the Government for excessive surveillance, but when it comes to the large cooperations they collect a lot of our data which is more than what is expected for the unique delivery of the service which we are in but we never question them. We question them but we are not left with the choice. As Jon said that it is about you using the services you have to probably buckle down to I mean the terms of the game and we probably accept it because it is always a tradeoff. If you want to use the service you have to probably give back something. So I mean is there something called real privacy? Are we moving away from privacy. I want to emphasize on that. And I also want to know from the panel what is their futuristic view of the Internet in 2030.

>> JON LAWRENCE: I'll jump in quickly on the privacy question. I think I don't believe it is. I think it is -- I think it is important in this point to be made at a couple of sessions earlier in the week, but I think it is important to remember that privacy is at the end all about you having the ability to make some decisions and exercise some choice about your data. I think those decisions and those realities still exist. They are clearly changing rapidly and perhaps narrowing rapidly as well, but I think from a more positive perspective I think the fact is that the general community is starting to become more aware of these issues. I think without necessarily praising them I think organisations like Facebook and Google have actually done a lot of work in this area that has been putting these things front and center of people's screen and saying come check your privacy settings. Whether they do or not at least it is sort of in their face and they are starting to think about it. And I think the other thing that's really starting to trigger people certainly in Australia is some of the advertising tracking that's going on. And some sort of

the creepily specific ads they see start appearing on websites. And people are starting to realize I can see what's going on here. And I think we see the rise of ad blocking, ad blockers around the world as not only a pretty existential challenge to the free public business and that sort of consumer we are starting to understand what's going on here. And we are not comfortable with it and it has to change. That gives me some hope.

>> A story to tell. I was at these Focus Group sessions. The first group was a dozen millenials, people in high school, still dressed in school uniform, observing them through two-way glass and they say they are concerned about privacy. But you put information about yourself online but don't know contact addresses or phone numbers but the case what we do is okay. The next session happened by chance to be people in their 50s, retirement, my age my friends and they said they were concerned about privacy. We don't worry. But secrets, ahh. We cannot let other people know. So both sides are talking privacy, but one concern is about secrets and one is concerned about personal data. IoT I think our secrets are still safe.

(Laughter).

>> SHREEDEEP RAYAMAJHI: I think that privacy is not dead. It is a socializing, you know. That's like something like technology changing, Internet is changing. So, you know, the core values, everything is changing. We need to adapt. IoT its that pros and cons. IoT can save lives as well. We have to understand that fact as well. It can be a pool for a disabled, for a heart patient or any other disease or disability condition. So it is just that we need to work on these issues with more focused multi-stakeholder concept. And we need to have more discussions and we need to work it, you know, in a more proper way. The Internet previously was just managed by technical communities. Right now it is ours. It is everyone's. So with that we have to accept open standards and move on, you know, just as they said it is there. We need to work on it with a proper approach. Thank you.

>> CHESTER SOONG: To answer your question I think first I think it is okay to have sometimes conflict in interest, in Government saying we need to protect privacy of the citizens but as well as, you know, doing works in terms of crime prevention, terrorism and things like that. I think the real important point here we need to have relevant legislations in place to counterbalance these acts and to set clear and solid oversight which is responsible to the citizens. And by doing that we need to have education and awareness would be important. So this is not really shifting the responsibility to the consumers or to the people. But really just to equip them better in that sense so they can question their legislators and question their Governments saying well, you are doing enough. Why aren't you doing that, you know, and when that comes along, you know, in fully Democratic society which I don't really have, I think I need to apply for the right to

be forgotten for the last comment. But the point is like, you know, in that system, you know, we would be able to make sure that happens. Because the citizens they are voters and in turn they are customers for the legislators to getting elected. So that's one way of ensuring their rights or their privacy rights to be assured.

>> ZAKIR SYED: I will keep it real quick in coming to your point, Mohit. It has never been the Government part of, you know, the thing only. This private -- the private part has actually been targeted. It is not only the Government who has been doing, playing actually with the privacy stuff. I mean, for example, the right to be forgotten in the European Union, these cookies policy in the European Union, the Google and the Chinese Government issue. So these big technology giants having issues related to cybersecurity and privacy things those are theirs, but at times there is stuff that is done by the Government which gets highlighted more times. So yeah, I mean the two will go side by side. And I really see them working together in harmony with each other to be able to realize a very, you know, productive and effective IoT environment for masses across the globe. Thank you.

>> SATISH BABU: I see privacy from two angles. First is the general public. But if you look at the bunch of people who -- for whose life depends on confidentiality, for them privacy has been dead for many years now. None of the existing tools, has been broken by several agencies. Torr is supposed to be the top in anonymity. There are some new tools coming up. There is no guarantee these have not been broken or they will not be broken. Plus most of these so-called companies which supposedly are kind of complying with the regulations have back doors. So if your life depends on please do not believe that privacy exists. You will be killed if you think so.

>> MOHIT SARASWAT: Thank you for all the panel members and wonderful audience. You have been really wonderful in all of the questions. And we think that you have enjoyed the session as we did. So I mean we will stop by probably applauding the panel members and the team here.

(Applause).

>> MOHIT SARASWAT: Thank you.

(Session concluded at 1532 p.m.)

***

***