FINISHED FILE

ASIA PACIFIC REGIONAL INTERNET GOVERNANCE FORUM
EVOLUTION OF INTERNET GOVERNANCE:
EMPOWERING SUSTAINABLE DEVELOPMENT
MACAO 2015
2 JULY 2015
ROOM 2
9:00 A.M.
SMART CITIES IN ASIA AND THE DEPLOYMENT OF BIG DATA:
PRIVACY AND SECURITY CHALLENGES
SESSION 9

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

***

***

>> NIR KSHETRI: Good morning everyone. My name is Nir Kshetri. I am from University of North Carolina at Greensboro. Welcome to this session on Smart Cities. And we will be focusing on a couple of things, big data and security issues and privacy. And we mainly focus from the Asian perspective of big cities. Supposed to be a 90 minute session. My colleague from Colombia could not make it here due to some logistical problems. Laura Lemire is here from Microsoft. She is a privacy attorney at Microsoft headquarters and her more detailed bio is online and we have -- we have divided this in to two parts. Laura will be focusing on the micro aspects of big data and Smart Cities and I will be focusing on the macro aspect of the Smart Cities. I will introduce the macro perspective and Laura will be focusing on micro.

The definition of Smart City or Smarter City. Smart City has a couple of these components. They utilize visual

technology or information and communication technologies. The goals of all those initiatives are to improve the quality and performance of urban services, reduce cost and reduce some resources and also the regulators and the Government want to have more effective and active engagement with the citizens. Those are some of the initiatives in Smart Cities.

And Smart Cities are already supposed to be something like a trillion dollar industry. And if we look at the cybersecurity spending on these Smart Cities it is something more like a billion dollars this year. That's why some of our sales companies are estimating. And Asia is very interesting from the perspective of these Smart Cities and big data because South Korea has more than 15 Smart Cities initiated. And Japan is doing a lot of things and China is planning to have more than 100 Smart Cities and India is planning to have more than 100 Smart Cities in the near future.

Another thing important from the Asian perspective most of the main technologies for Smart Cities they -- Silicon Valley and all those different places but these could not be implemented in the U.S. because U.S. people or the European care more about data privacy. It is data privacy is very important for them. And Asians care less about data privacy. And because of that the U.S. technologies are first deployed in Asian cities like -- new city near Seoul. That's the first Smart City they built from scratch because of the Asian more friendly environment from a data privacy perspective. And another thing about a Smart City is that okay, there is a lot of data collection initiatives, privacy security issues and what's interesting data, data collection initiated through the service. If you look at examples from some of the African cities like Ethiopia and Egypt's Cairo, Government regulators and Governments are collecting a lot of data and use for -- data of the citizens and that is possible also in some of the Egyptian areas. Some of the issues that I will be focusing on.

Okay. Let's see, actually this is about Smart Cities and one estimate is -- so this thing that by 2025, 58% of the world's population will be living in Smart Cities. That is something like more than 4 billion people all over the world. And if you look at South Korea there are more than 15 U cities, and an example is the New Songdo city, that's 2030 held in New Songdo city, two years back and I was at that conference. And New Songdo University is the only one, only Smart City which is built from scratch. And other Smart Cities initiatives are basically smartizing the existing cities. And this is a 45 billion dollar project. And mainly the U.S. builders and U.S. technological companies like Cisco and IBM and Microsoft, too. A lot of U.S. technology companies involved and also China has

planned to build more than 103 Smart Cities and India's Prime Minister announced plans to have more than 100 Smart Cities and also Saudi Arabia is investing more than 70 billion U.S. dollars to smartize the cities and also in Singapore, Hong Kong, Dubai, a lot of European countries. And also Japan is working a lot in 2004. Because all this thing one estimate for the sales company is that global Smart City market would be more than one and a half trillion dollars by 2020. And also privacy and security issues are facing Smart City is very important because these Smart Cities initiatives are focusing on other things like the functionality of the technology. They are testing for the -- for the -- all the components that they are using but Smart City initiatives are not focusing a lot on things related to security and privacy.

And also they use very sophisticated features in those Smart Cities and functionality and because of that they are very vulnerable to different types of cyber attacks because of a lot of different characteristics. And there is a lot of different types of technology like the broadband, WiFi and all those things provide an entry point for hackers, and also if they are able to hack one of the components, one of the devices it is easy to enter other things because those other devices, other systems think that those -- those communications are from the Smart Cities and they do not resist that type of -- that type of attacks.

And also we already talked about that. And another thing is that if Smart City experiences, cyber attacks, that is likely to have more serious consequence to victims of the Smart City and also to the society. Because of a lot of information, Smart City involves a lot of data, big data. And also they rely more on technology. They rely more on technology and realtime information. And if there is no city -- light is not working or the traffic light is not working, it means they don't know how to manage things. So over (inaudible) is a problem. They talk about all the cybersecurity experts about let's say cyber attack versus nuclear attack and the argument is that no one has guide of cyber attack or cyber attacks do not pose any threat. That is one argument. Given that there are already some cyber attacks which have been able to cause physical damage, if you look at the nuclear power used in Iran and already in Germany and other places where they cause physical damage, it is possible in the future that cyber attack on the Smart Cities might involve even those physical damage and other types of problem.

So because of all these things, these Smart Cities have been spending a lot of money on cybersecurity and this year according to the Pike Research more than 1.3 billion U.S.

dollars will be spent in cybersecurity involving Smart Cities.

And also looking at the privacy and security issues, surveillance and data surveillance it is kind of tracking the trails, created by a person's activity. If you look at the New Songdo University that I talked about they have a smart card. They can ride the bus. They go to the movie theater and watch movies. They can visit museums and one smart card can be used to do anything, and because of that if the Government has access to the information with the smart card or a hacker has access to the smart card they know everything about the citizen. So that is one problem. And also not only from the cybercriminal's perspective also from the authoritarian Government or even the Democratic Government who are interested in spying on citizens, it is very easy for them to do that. That is one problem. And to take one example China is working a lot on smartizing cities. They have rich initiatives in Beijing in 2011, information platform of realtime citizen movement. That's where the Chinese Government in Beijing started in 2011. The distinctive goal of the Government is to tackle by monitoring people. If you look at Human Rights activities and their argument is the Chinese Government might be using, that information to separate activists and that is a problem that they have. And in many authoritarians those Civil Society and citizens they have less power and Brazil has a lot of Smart City initiatives, and in Brazil which is a more Democratic society, they are starting with Smart City initiatives in the Rio de Janeiro. But in authoritarian city they do not have a lot of power. That provides more opportunity for the Government to control on citizens' activities.

And also looking at some of the key issues in Smart City initiatives, also we talked a little bit from the Government's standpoint. Also from the cybercriminal's standpoint there are a lot of issues related to privacy and security. Because Smart Cities are -- have a lot of data and those data allows cybercriminals or the Government to monitor the movement of residents and create their profile and information can be shown in the underground market. This example is from China. Actually if you have switched data that's in China but those database can cost something like -- buy from the black market for $1500. And you have the data. Can use the data and they charge the French as much as $150,000 for the data and the data -- the resource in China indicated that they buy on underground market. They can be used for private investigation or asset investigation. So these types of things already exist in China and other parts of the world. And this problem becomes more serious in Smart Cities because data is more valuable. And also Smart Cities use people and centers and we do not know who is

the receiver. And the receiver of the information from the center is a back actor. We don't put a lot -- we don't know a lot about the trustworthiness of the receiver and that might be some type of adverse consequence if the receiver uses that information -- okay. Next one. Sorry. Thank you.

Okay. Another thing is these malware virus and all these have limited. They have been here for 30 or 40 or 50 years targeting all these computers and cell phones and all these things. But malware targeting the systems used in Smart Cities are very, very new things and the newness, these are new things. And we are not mechanisms, defense mechanisms. For example, in the industrial system might cause physical damage. These are not from the Smart Cities because Smart Cities are very new. But this is actual examples of malware and worms causing physical damage. I have these examples of which to illustrate that this is a real possibility, physical damage of residents and people of real possibility in the future. You might be familiar with Stuxnet malware used against the nuclear power plants which use self-destruct and overspin and also the console, showing that the New England processing plant was operating at a minimal millimeter and all these are examples of malware causing physical damages and probably don't have to talk about all these things. So the idea here is that it is a real possibility. Physical damage is a real possibility.

And also another example that -- more recent example was the black energy and black energy also exploited the industrial system which was exploited by Stuxnet and another example was 2012 Shamoon malware or worm in Saudi Arabia, biggest chemical facilities in the world. 30,000 computers and hard drives were wiped out which was 85 percentage of the company's computers. And also it tried to attack the Network which display hardware international supplies and exploiting other hard drives. And in 2014 December Germany's federal office for information security, BSI, and they were reporting that hackers caused physical damage to a steel plant in Germany, spear phishing and social engineering and also penetrated the products. Examples to illustrate physical damage. Possibility of physical damage that exist in future and which has more serious consequences in the case of Smart Cities. Next slide, please.

And also Smart Cities are our -- utilize -- a lot of Internet of Things and Internet of Things, Botnets are becoming more and more prevalent in recent years and the first example was from about two-week period from December 23rd to January 6th of 2014, December 23rd, 2013 to January 6 of 2014 and the Botnet exploited about more than 100,000 connected devices and about 750,000 sent over 100,000 devices of Spam. Anything can break in to one device. Or anything connected to the Internet of

Things, Smart City, like heating, lighting, vending machine, security, WiFi, device, Smart TV and it is easy to penetrate in to other devices. I think the communication is coming from internally and they do not resist that type of thing. Building the SCAD which is supervisory control and data systems and these are the ones that are used by many Smart City builders for managing facilities and also building operational needs but research recently in the past three years has indicated that all these systems caused big vulnerability factor. Because these are used to upgrade energy infrastructure and also -- also operating to richest components, like Frost & Sullivan and all of them have done research to indicate that these systems pose major cybersecurity threat.

Next. Go to the BAS, which is the building automated system that we talked a few minutes ago. This BAS definition here is BAS. This is a centralized internal link of hardware, software, monitoring and controlling environment in commercial, industrial and institutional facilities. In the U.S. only -- this is a little couple of years old data. More than 15,000 BAS systems are in the U.S. which are accessible by via the Internet. And two years ago about 90%, more than 15,000 BAS used in the U.S. were to have some type of cybersecurity related vulnerabilities. And one problem with BAS is that they are vulnerable 24 hours a day, 7 days a week. They are on the Website. They do not have security measures and they do not have those systems that often and because of that they pose high degree of vulnerability to the cyber attack.

And also insiders criminals and Botnet operators, all those players, and we already talk about the attack from insider because of that easy to penetrate internally to other things. Yes. Next slide, please.

>> Oh, sorry.

>> NIR KSHETRI: Thank you. One before that. One before that. Sorry. I think that's stop. Some examples of the building of automated systems, cybercriminals targeting that system and this comes from the U.S., from the Department of Homeland Security in 2013, April. According to their study hackers were trafficking the energy management center connected to the Internet and basically they were able to manipulate the lighting and heating and air conditioning and also they can unlock the door and turn up lights using those vulnerability used in the system. And this is important because research has indicated that if the temperature of a facility is increased by five or six degrees they cause the malfunction of the computer and the process those transactions at normal rate. The cybercriminals were -- they can damage the data. Just by turning of the key. This is a serious problem.

An example of another thing is that Tridium company has Tridium software. They use for the building. In 2012 research indicated that cybercriminals can use the vulnerability to open garage door and front door and penetrate the computer network and these are two examples from 2012. And these hackers were about to exploit the Tridium vulnerability. In one example the manufacturer, New Jersey manufacturing company, the New Jersey manufacturing company was accessed from the Internet and another state Government facility, the state Government facility was changed using these vulnerability of the Tridium software in 2012. We talked about key issues related to privacy and Smart City initiatives which are some of the possibilities in the future. And also this is mainly about big data we talked in the beginning. So before that probably I will make a comparison of how other types of cybercrimes and cybercrimes, cyber attacks targeting Smart Cities might have some differences. And so I have compared this with some type of cybercrime that many of us experience these days. Sorry, next slide. Sorry.

Okay. So I just make a comparison here between identity theft and cyber attacks targeting the Smart Cities. If you look at the first, I think it is kind of no level of seriousness. Maybe a couple hundred dollars or Social Security number or all these things and they have -- similar to the cyber attacks targeting Smart Cities they may not be -- they don't have serious problem. And the perpetrators in the I.D. thefts might be the criminals from the Nigerian, those thieves and those are the cybercriminals involved in I.D. thefts, but if you look at the Smart Cities that are attractive targets for cybercriminals because there is a lot of information for terrorist and also for adversary Governments. Smart City built from scratch we talked in the beginning was the New Songdo city in South Korea which is only 30, 40, kilometers from the North Korean border. A cyber warfare has been going for the last few years and if the South Korean Government loses -- and if you have the -- how those perpetrators operate and there was really older, like 10, 15 years old, some of the malware were new but mainly they are using the established from all malware. But in the Smart Cities the malware and all those things are completely new. Like I would be Botnets or BAS Botnet. They are completely new phenomenon and because they are new we do not have any defense mechanisms or the cybersecurity companies have not come up with any new defense mechanism.

So new people are already aware of the I.D. thefts and they know how to take the technological, behavioral and cognitive defense mechanisms in the established type of cybercrime but the defense mechanisms have not been very well defined in Smart City related malware. And there is guidance to configure the

Internet of Things and also device mechanisms, and Governments and organizations they haven't paid enough attention to cybercrime related things in Smart Cities.

Okay. Now we talk about big data. Everyone is talking a lot about big data and first what exactly is big data. And I have done some research in the past couple of years about big data. And so based on that I have combined these five things about big data. The first three comes from sales company and the last two vary in complexity of those two characteristics of big data come from a technological company based in North Carolina. So I combine those definitions of big data and companies of definition of big data and examine how those characteristics are related to cybersecurity and privacy in the complex of Smart Cities. First of all, in big data has a lot of data. And IBM Watson that every day we generate more than 2.5 quintillion bytes of data. I did not know a couple of years back that's ten zeros and 90% of the data was generated in the past two years. And data comes from a lot of different sources, like a lot of transactions that we engage in, voice, coming from everything. And, of course, the Smart Cities involve more big data, compare other types of initiatives and because there is more data, more data means more attractive to cybercriminals, more attractive to the authoritarian Governments and not only that some data, for example, all these Smart Cities they use smart meters and results has indicated that the data from smart meters are high data, in the sense that the amount of money that the utility companies get, the data that is transmitted by the holding of data that is transmitted by the smart meter many more times than the utility companies give from the (inaudible). Because the smart meter data generated by smart meter using that data they know exactly what devices are using in your home and what medical devices you are using. Based on what medical devices you are using, what kind of notices you might need and this might be -- some data high and by example that I gave smart meter data.

So a lot of data attract cybercriminals and hackers and Government. And complexity means -- the idea is that data are to be collected quickly and analyzed and processed quickly and based on the data you have to take action quickly. And compared to other types of cities people rely more on the past data. One example is a traffic light. Traffic light means it is based on the real movement of people. If the traffic light is not working then there might be more severe consequences but you are relying on the realtime data and realtime data means that the realtime data is not working or it is manipulated then you might make action and might have more severe consequence. There are structured data with our mainly numbers and also there are more

unstructured data. Unstructured data coming from the maybe audio, video pictures, all the unstructured data and all these companies or cybersecurity companies know one of two things about how to protect structured. But research has indicated that many companies do not have mechanisms to protect the unstructured data. Like more importantly unstructured data like your picture or video has more personally identifiable information. And if the security violation takes place there is more severe consequence with the unstructured data. Variability means that data flow vary over the time and kind of slow period, not a lot of data comes. And many companies can manage data only on the -- there is the regular amount of data flow and peak data flow means more data and more data is more attractive to cybercriminals.

In the U.S. there is the big utility company target which lost information of maybe 70 million people in the -- and the criminals are targeting in the big data flow period, from something like ten million to five local time because targets, to allow some of the transactions. And so those are the times that criminals might focus on a lot of data flow and complexity means data are coming from a lot of different sources which is called linking data, natural data, transform across system. And one problem with that is data is coming from everywhere. Like from the trash can smart meters and you might think that data is anonymous. Researchers have found that new anonymous from three or four sources they can combine those data and they can basically identify whose data that is. So they have that -- they have been doing that. The characteristics in relation to cybersecurity and privacy. So those are some of the things that we talked about in Smart Cities, mainly from the Smart City as a global trend and maybe Asia, Japan, China, India, South Korea, Singapore all these countries, Asia have those Smart City initiatives and actually and originally from the Nepal and big earthquake.

Last week -- I come from Nepal. They were saying the future plan a lot of buildings were damaged. So they think that we should build a Smart City in the future. So some type of Smart City. Not like the New Songdo city in South Korea but some version of Smart City. So Smart City initiatives are everywhere in these Asian countries. We talked about cyber attacks on Smart City more deeper consequence and surveillance and activities and programmes they are more likely because of the automated and Network technology and privacy and cybersecurity awareness. In Asia it is very low. Asians don't care a lot about privacy and especially the countries like India and Nepal and all those countries in Asia many people are using advice let's start using the cell phone and computer and they

don't know a thing about cybersecurity. So it is very important to educate with consumers how the information is working and why is privacy important and why is cybersecurity important and also from the cybersecurity and privacy standpoint. We have not had both the things what is the reality and what is people's perception. Those are the two things that we have to look at and also going back to the New Songdo city in South Korea. That is the only Smart City in the world which was built from scratch and the core technology was housed in Silicon Valley. And they couldn't do that in the U.S. Because in the U.S. we care a lot about privacy and South Koreans don't care about privacy. And that's why they have to bring in South Korea and they used to automate and monitor everything in that city. And -- so that anything is not possible in the U.S. And Palo Alto is one of the companies that developed the key technologies used in the city. Historically there is less privacy in Asia. Computing is controversial in the west and many countries in Asia like Korea and other nations in Asia they consider the new computing as a personal investment as well as domestic and actually living in Smart Cities or using the latest devices. And those are considered to be more prestigious things in Asia. They use these technologies to show other people. They are concerned less about the privacy issues and privacy, if you look at the European Union countries and even to some extent in the U.S. there are clear laws regarding how data can be collected, how they should be stored, how they should be reused but this is a new thing here. And also if you look at the Gulf countries like the United Arab Emirates they have developed a Smart City. And Saudi Arabia is investing more than 70 billion U.S. dollars to develop Smart Cities and dictators have been using the Smart Cities, like the technology from the surveillance and data mining. And the goal is to control over terrorists, a lot of criminal outfits and also minority groups and also the migrants. They are using these technologies. We have less experience from Asia but this is a possibility in Asia, too. There are these large views and interest internationally. So one size fits all type of thing doesn't work. So the type of system that might work in the U.S. or Europe may not work in Asia. A lot of people possibly be perfectly controlled, perfectly efficient, safe Smart City and the example is New Songdo and that might function like a machine and may not protect privacy. That is working on -- may work in Asia but may not work in the U.S. and European countries.

And also societal things we have to look at in these initiatives and in that interest primarily served by the data gathering initiatives like the authoritarian governments in many of the Persian Gulf regions are using those data to control over

terrorists and criminal outfit and the minority that we talked earlier. So okay. The idea is that there are these alternative models of Smart Cities. Might be able to use completely centralized or some degree of recentralization. And so probably the (inaudible) and the technology developers and Civil Society might have to engage in cross national and cross cultural components related to big data initiatives.

And thank you very much. But if you have anything you would like to ask me, that may be a good idea to do first and then Laura will be talking more micro thing because Microsoft is one of the big players in Smart City and technology. If you have anything we can maybe talk first or at the end. We have a lot of time. Looks like no one has anything to ask first. You can go now. And thank you very much and maybe we discuss at the end.

>> LAURA LEMIRE: How many of you were familiar with Smart Cities before this talk or how many of you are having the Smart City movement in your town where you are from? Great.

>> NIR KSHETRI: Okay.

>> LAURA LEMIRE: I will go through now. My name is Laura Lemire and I'm an attorney at Microsoft. I am fairly new in the Smart City open data movement. My primary job is to help engineers design software on our cloud services so they work for our customers. So -- and I primarily work for -- work on enterprise services and software. So I look at the types of privacy and security regulations that might apply to our customers. So, for example, banking regulations in Singapore that might impact our customer's ability to use our software or our cloud services. And then I also look at the regulations and privacy and security worldwide that might affect the way we design our cloud services. So I was brought in as part of the Smart City open data team at Microsoft that are thinking about these issues. Because Smart Cities we hope to be our customers and thinking about the privacy and security issues that cities might have.

So today I want to talk about why Microsoft cares about this. I will mention some of the -- Nir Kshetri did a really great job giving us -- giving us a great perspective on privacy and security issues, but go back to some of the things that are driving the movements and some cool solutions that can be available to solve some of the problems that cities are facing. And then I will talk about the security and privacy risks. Again I would like to talk about the kind at the micro or street level. I think talking about smart data and Smart Cities is fun. It is an interesting way to use your imagination to think of the scenarios that can happen. So we will talk about the privacy and security and talk about some of the things that

Microsoft is doing. And again here I would love to get your feedback. If you think there are things that we can do or guidance that we can provide, I would love to hear from you on that.

So first let me talk a little bit about what's happening at Microsoft. Microsoft is 40 years old. It is interesting if you look at the landscape of people in the tech industry. Google, Google is about I think 17 years old. Tanzen is ten years old. Facebook is not very old. We are probably one of the most experienced countries. And we are changing and trying to use some of the wisdom we have. We have a new CEO. And I have been at Microsoft for awhile and there is an era of change. A lot of the things that, things that we would have never done, embracing open source and working with competitors. We are definitely doing all those things and we are all focused on on our current mission which is that we want to help every person on the planet do and achieve more. This is where we come to care about what's happening with Smart Cities.

So let's look at some of the problems maybe. There is a lot of things happening in cities right now. The fastest growing cities are in Asia. And the most urbanization is happening in Asia. So the largest urban growth will be taking place in China and India. And we need some sustainable development, right? There is a lot of problems that come with those, with all of that rapid, you know, rapid population increase. Tokyo has 38 million people. In Delhi there is 25 million and expected to take over Tokyo's population. What can we do to have sustainable development in those cities? There is transportation issues to think about. Food issues to think about. How do we make sure people aren't going hungry. There is sanitation. There is environmental issues. There is utility issues. And all of those things present some really hard problems but also there is technology now that we can use to really solve those things. We talk a lot about the problems with Smart Cities but also that huge promise, the innovation that we can have that will make people thrive in cities and improve the quality of life in the cities where there is so much population growth. And then in addition to the demand for Smart Cities there is also a number of things happening that is really bringing an appetite for change. You have got people -- yesterday I sat in a session where they were talking about how they are increasing skills, getting increasing digital literacy and people in Asia. And there is a hunger, people want to use technology to solve problems and there is a lot of work that's happening with white spaces to get Internet access in places where it hasn't been possible before.

And there is a lot of interesting and political attention

to, you know, having smart sustainable cities and transparency. So in a lot of places people want more accountability by their Government. Where is the money going. What's happening. People are actually wanting more data. They want to see what's happening. So all of this is creating kind of this environment where there is a lot of need for innovation. And you know what, there is people and activities happening that can make it possible. It is a really cool time.

So let's talk about those -- the security issues. So first there is a lot of unique things happening with Smart Cities. Let's talk a little bit more on a street level. What is a Smart City? So let's talk about a city that's looking to do really smart things with transportation. So maybe that means they have devices on every traffic sign. They might have cameras around the city so they can actually look at where people are going. Maybe they have sensors on park benches so they can monitor foot traffic. It is a number of different types of devices and there are many of them. So that really presents a unique challenge. So first how do you secure that? It is different. You know, when you talk to some security people they think about servers and locked rooms and locked cages where we train people. They have security training and we put locks on the cages and we change passwords. But how do you secure this where you got sensors all over the place. It is really a unique problem and they are all streaming data. There is some limitations with that. If you have a device that's on a park bench is it capable of encrypting data. That's an issue. Just the capacity or the potential, the computing power that's on that device. So that's an issue. You know, it also is -- there is so many devices and so many vectors. How do you know -- it is not like you can put all the servers in one room. You are talking about devices that are all over a city. So it really presents new challenges and it gives people that are on the security space a whole new world. It is a whole new ball game as far as securing the data and securing those devices. And then there are -- there is the same problems that we have with traditional software. You have vulnerabilities. So what happens when a vulnerability becomes known and software that's running the water supply for a city, right? What types of policies need to be in place to ensure that, you know, that vulnerability isn't used or that it is closed very quickly. Those are some really unique public policy issues that we have to think about. And then, you know, there's some -- there is other things that we have to think about, too.

You mentioned a lot of attacks scenarios. So what happens when somebody can -- they can control the video cameras that are being used to monitor traffic and they can plan a crime and see exactly where the police are going to show up because they have

access to what is happening on all those cameras. This is the fun part to imagine all the weird things that can happen. I think it is a little kind of interesting. So this is, you know, really coming up with some unique security challenges. And finally there are some new threats. In addition to vulnerability and insecurity and there is the physicality. How do you create the Smart Cities so that it is prepared for huge rainstorms or earthquakes or any other things, physical things that can happen. Those will definitely have to be part of the plan when you are thinking about Smart Cities and Smart City security. Having backups, if you have a Smart City system that's controlling the water supply and it goes down, what's the backup plan? Have you thought about it? How will you continue to give people in the city and community clean water? So those are things that I think come to mind for me when I think about the unique security challenges with Smart Cities.

And then there are some unique privacy concerns. So I know that the privacy laws are not as far developed in Asia than they are in Europe or even in the U.S. And in the U.S. we don't have really robust privacy laws but I don't think we can say that everyone in Asia, you know, nobody cares about privacy. I think that everyone cares. And actually there are these principles that we come to think about what we talk about privacy. So a lot of them come from what is the OECD principles which were developed in the 1970s, early 1980s, and OECD is the organization for economic -- what is that? I wrote it down. Sorry. Economic Cooperation and Development. Japan, Australia, New Zealand were part of this. These are principles that we think about with privacy. The notion of consent. So under these privacy principles which are embedded in most of the privacy laws around the world. There is this concept that you have to get people's consent to collect their data and use it. You have to tell them what it is going to be used for and you have to get their consent.

So how do you do that when you have traffic cameras or you have, you know -- you have sensors that are monitoring your license plate on your car? How do you -- can you consent to that? You really can't, right? So there is this really -- there is a way that these fair information principles that are being completely uprooted by the Smart City movement. What takes the place if we can't get people's consent? If we can't make sure they agree to what is being done or can't tell them what the data will be used for. We think the data will be used to control traffic but we might later find out that we can use the data to maybe solve a public health issue or something else. A secondary use of that data collection. How do we get consent? So one of the things that we have to think about is what do we

do now. And I think one of the things you will see is you will -- you will have to have increased transparency about the data that's being collected. It will be really important in these cities that people are aware of the data that's being collected and how it is used. And I think that people are going to want to have some access to that. More open data movement and I think that people will want to be able to control the profile on them. So maybe there's a list of here's all the things that we know about you, Laura. We know these are your patterns. I mean -- maybe I can delete some of that. So I think you are going to see a lot of push for transparency and some control over that data.

And then the big data possibilities, so we talked about a lot of some of the scarey things that could happen with big data but there is a lot of really cool things that can happen. One thing at Microsoft this isn't a Smart City example but we took anonymized search results and we found people that were looking up a drug for cholesterol and they were looking up -- and then we took people who looked up a drug for cholesterol and people that were looking up a drug for I think it was blood pressure. And then we looked at people that looked at search queries for both types of drugs and we found that people that were looking for both types of drugs were also searching for stuff, medical issues they were having that were symptoms of diabetes. So just looking at the search query we were able to find out that the two drugs taken together can cause diabetes. That's not medical research. Google you can find out a lot of cool stuff that you can do with big data. Big data possibilities are really cool but they are also kind of scarey. There is the Target example. Target was able to determine that the department stores in the U.S. they were able to determine that people who buy cotton balls or unscented lotion there's a probability that they are pregnant and they can start sending them coupons for diapers. That was something -- it was unexpected. So can, you know, can the Government find out, you know, looking at my traffic patterns that I'm going to change jobs or that, you know, maybe something else, maybe something else about my health. So, you know, what's interesting about big data is when we collect the data we had no idea how it can be used and that's both really promising and also very scarey for a lot of people.

And then there are fear of tradeoffs. So with all of the Smart City innovations there's going to be the fear of what does this mean for our individual freedoms or personal rights and what people care about the most will vary depending on what country or what your culture but in the United States there are many people who are worried about surveillance and Microsoft is really worried about that. In the United States we have the

right -- Government can't do unwarranted searches and seizures. Is it a search and seizure when Government has access to some really interesting information about my patterns without my consent? What does it mean that you -- you are constantly giving the Government access to your information?

And, you know, privacy is a component of -- we thrive with some level of privacy. It is great that people can't hear our thoughts. We are worried about people being able to predict our behavior. There is a lot of fear what are the tradeoffs of Smart Cities and we talk a lot at Microsoft. Our CEO has mentioned how do we maximize the technology and preserve timeless values or important community values. So I think that's going to be something that we all need to think about as we become part of this.

So we are thinking about how do you make cities thrive. So we definitely were reaching out to cities and we are creating partnerships. So we are working really hard on that. There is some people at this conference that have mentioned some things we have. We have city next, we are doing some training. So there is definitely a lot of things happening in partnership with local offices and cities.

We are trying to connect communities with some tools. And we are making a lot of tools available for free. I am trying to get research or provide guidance to communities that will help them make this next step and use the innovation in a way that will help them thrive and this is definitely where I love to hear your feedback on the types of things that we can do to help cities really enter in to this next phase.

So here are some of the tools that we have. I work on some of these goals, I work with the engineers. Power DIT, a Microsoft product that a lot of people haven't heard of but it is a way to visualize data. Make sense of the big data. It is not a lot of people have heard about it. So I always like to mention products that I work on that, you know, my mom doesn't know about or my friends don't know about. And then we have got business spark, fuse labs and Microsoft adventures. These are trying to help small businesses to get off the ground and then some of our other programmes. So with that thank you.

>> NIR KSHETRI: Thank you very much. Let's see if you have anything to ask Laura or myself.

>> (Off microphone). I recognize all the things that (Off microphone). So I am fully aware of all the (inaudible) and Networking (Off microphone). But the other thing that appeared to me is that a lot of us tend to come pretty much from the computer and Network perspective which is natural. But the one thing that sticks out for me, when you are talking about (Off microphone) and the wireless and engineering safety culture and

the other one is, you know, (Off microphone). This is really where safety and security in a lot of cases are alike. One of the problems is especially master control systems is they often have been designed on the basis of safety. The idea that you certify every component of those and once it is certified you don't change it. So the security game when you are in the Networking world it is patch, patch, patch, patch, patch and in the engineering world (Off microphone) about research, research and for a lot of businesses that's simply quite expensive. And work going on, especially in North America where people are waking up with the idea that hey, I am having (Off microphone). And, you know, from the business side of things a big opportunity (Off microphone).

And you have got -- (Off microphone). And we have recently stopped supporting XP. (Off microphone). From an industrial engineer's point of view, it is an initial security system. I have to get my entire country certified (Off microphone). So my question really in this how do we bridge that divide to a lot of legacy systems and culture which basically requires them to go slow and (Off microphone). And the requirement to basically be (Off microphone). We all know that there is no guarantee that some (Off microphone).

(Laughter).

>> NIR KSHETRI: Microsoft.

>> LAURA LEMIRE: You know, it is a really big challenge right now. For us we got -- I was at a conference about a month ago and a customer told me that they had a medical device running I think on a Windows 3.0 or something and especially in the health care industry they make these huge investments and they don't want -- they couldn't get off the technology. For a company standpoint it is hard for us to continue to support products and then move to new stuff. And we're definitely changing. We actually just retired patch Tuesday which is a big change. And we are actually launching a Windows 10 soon which is different. It is going to be a service. It will be very interesting. So, you know, we are -- we provide patch support for -- you might know better than I do. I think ten years. And at a certain point we have to focus on the current product. So it is a problem that we have and we have programmes to help people move on to new technologies. But again it is -- it is going to depend on the customer's needs. They might be, you know -- they might not want to change. So we're definitely looking to the future where, you know, we will make it easier to keep software up to date. But, you know, we are also thinking, you know, we are aware of those customer's problems. It is just -- honestly it is a really hard problem to solve.

>> NIR KSHETRI: The person in the back.

>> My name is Tom Hollander from Brook Haven. First of all, what was your favorite -- what is your favorite science fiction books or (Off microphone). A hundred years ago when I was in school instead of reading text (Off microphone) science fiction books and (Off microphone). Fahrenheit 451, scoping process. (Off microphone).

That's the first thing. But another thing to ask, the second point I would like to -- with respect to you said there was a need for consent. This came up at the APrIGF last year and we had a room full of young people. They were probably 40 or 50 people from local schools that brought up this issue of cyber bullying, a whole host of things and they talked about their cell phones and their Smartphones. And every one of them knew they had consented to the application's requirements. But they didn't want to actually share their data but they wanted to use the application. So it was -- it was a conscious decision, that said yep, because I want to be on Facebook or I want to be on Skype or whatever the latest thing is. They said yes, but I don't know that it was a full consent. I think it was more a perused consent. They wanted to be with their peers. (Off microphone). Bring that message that came out from last year's APrIGF and back in to the same thing in this year. (Off microphone).

>> NIR KSHETRI: Would you like to answer, Laura?

>> LAURA LEMIRE: Hmmm. Let's see.

>> NIR KSHETRI: I just write.

>> LAURA LEMIRE: I really like the Hunger Games series. I really like contact. I guess that's one of my favorites. I don't know if those are relevant. But I also like just reading about the technology that's coming out. I mean it is not -- it is not so -- to me it is really fascinating. One of the things that I am really fascinated by is the development of smart cars and autonomist cars and that feels like sci-fi to me. I recently read an Article about the ethics with smart cars where a developer will have to programme decisions that will get made if there is a crash. Are they going to crash in to the car or maybe there are children in the car and a car that there are no children in the car. There is going to have to be ethical things in the software code and I think that's fascinating. I guess I'm more reading about current developments. Privacy and issue with consent, it is definitely a huge problem right now. I think, you know, I think all of the different -- I guess kind of like the different environments, so Apple has their environment. And Android has their environment. Everyone is taking a little bit of a different approach and Microsoft we are trying to focus on giving people meaningful choice and control over their data. We have some things to do but we are

definitely focused on that. It is really tough. Right now the industry and regulators are focused on giving notice. So what does that mean for most companies? It means that you provide these really, really long privacy statements that nobody reads that are written by lawyers with tons of education, especially in countries where there is literacy problems that's an issue. So, you know, I think part of the digital literacy that's going to have to happen is awareness about privacy. What's being collected. What are you putting on the Internet. I think that's going have to be included in part of the education for kids. And a lot of people, they are not aware of what tradeoffs they are making with the use of some of these apps.

>> NIR KSHETRI: Back, gentlemen in the back. He is first.

>> (Off microphone).

>> NIR KSHETRI: Okay. One big challenge in Smart City and that is more serious and bigger version, the thing that we are talking about because things are a lot bigger and in the case of ad, deliver optimized ad based on who you are and what activities you are engaged in that may not be that serious and may not have those possibilities of physical damage or not very serious consequence. But because Smart Cities involve a lot of data and we rely on them a lot. Any type of privacy violation or cybersecurity threat that might have a more serious consequence.

>> LAURA LEMIRE: I think that Government participation is really important. It is going to be our tax floors that are funding this. So I think that people that don't trust what is happening they are going to ask a lot more questions and demand more different types of technology. I think that -- I think there's going to be real, you know, real -- if people don't trust the technology they are not going to want to use it and I think, you know, it is going to be really important to have people participating in the Smart City movement and asking for transparency. Where is the money going. How are you selecting venders that are, you know, what venders are getting access to this data and what are they going to do with it. How are you deciding which senses are better and which aren't. All of us should get more involved in that.

>> NIR KSHETRI: That is exactly the problem when you are working on Smart Cities but in Asia, like South Korea those people trust companies with their data. It is more bigger problem in -- from the trusting of technological providers and Government and public engagement and that is more serious than Latin America or Europe (inaudible).

>> So first of all, I want to say (Off microphone).

>> LAURA LEMIRE: You know, in the United States there is a Computer Fraud and Abuse Act and there is a lot of interest in

updating that. And actually I see it at the state level, too. There is -- states are trying to implement Computer Fraud and Abuse Acts. And, you know, one of the things, you know, in the United States and as other countries are implementing these types of laws, you know, I think it is really important to think about, you know, what's the intent. What's the intent of these activities. Was it malicious. Was it nefarious or, you know, was it in the research or whatever it was. I think that's going to be really important. And I think, you know, we'll definitely see a lot of change in that space. What is it. What's a crime and what isn't. I think there is a lot of, you know -- I think there's probably a lot of scenarios that Governments and law makers haven't thought of. And so, you know, I think, you know -- I don't know. I think it is an active space right now definitely. So I think that Governments are thinking about this. I don't know what -- I don't know what the best legislation would look like or the best law would be honestly. Because I'm not sure what the crimes will look like down the road. Again it is another activity where you can use your imagination to kind of think of things but we don't know all of the scenarios.

>> NIR KSHETRI: That's true. A little bit on Laura's point. He came up with some executive (inaudible). One of the main points, actually the proposed legislation rather and one of the main points is to amend the Racketeer and Computer Abuse Act. Identify cybercrime. But a lot of Civil Society people have law enforcement people like abuse that and also the language is very, very vague. That means if you share your Netflix password with other people and family members and then they can be put in prison for 20 years. Those are the concerns and they are still debating. It is still not a law but a lot of discussion going on there. Any more questions or comments or feedback?

>> This is temporary personal information for computing, people always feel the personal data, hope that Government can exchange it for personal information. So this becomes difficult when persons use this data. So we (inaudible).

>> NIR KSHETRI: So the problem here is --

>> Personal information.

>> NIR KSHETRI: Right. Okay.

>> People feel this information (inaudible). So people hope that Government was changing for this information.

>> NIR KSHETRI: I think this is a kind of serious problem now that the regulatory governments have not taken place, very vague. And many business it is currently (inaudible) approving in the gray area and it is not legal, illegal and (inaudible) are busy with other things and because of activities from the

interest group and Civil Society and principles and maybe more regulatory development might take place or even businesses like give you money for using the (inaudible). Right now those things are operating in a gray -- relatively gray area.

>> LAURA LEMIRE: Definitely if you look at the number of privacy laws that were enacted in the 1990s and the 2000s and even in this decade they are skyrocketing. So I think that regulators and law makers they are definitely interested in how they can protect communities and their citizens from, you know, invasion of privacy. And I think what you see is the laws really vary around the world. But they all are definitely -- they include these principles of notice and consent, transparency, giving people access to their data. So you see -- there are a lot more laws but I do think that it is becoming increasingly more challenging to -- for regulators and law makers to handle some of the newer issues that are coming out with the technology. So it is an area that's actually changing really rapidly.

>> NIR KSHETRI: Any more thoughts? Any more comments?

>> (Off microphone). You need to satisfy all those and support (Off microphone).

>> LAURA LEMIRE: So we hope everyone in the world will use our software regardless of where you are at. So we have to take all of the laws around the world and synthesize those and make products that are going to work for every type of customer and a lot of that means that we put in a lot of functionality that you can control your information. So, for example, you know, in Windows you can control how much telemetry or information that you can control if you send your crash data. There are controls on that and I think you are actually seeing a lot of companies respond to customers' demands. So Facebook is continually -- they have made a lot of changes to your privacy settings because their customers really want it. So, you know, it is interesting that companies are responding more to customers, more quickly than they -- than laws are being put on the books in some cases. So, you know, there's also as people want more privacy I think you will see people making products for that. So you definitely see -- you see these new apps being developed that are -- you see -- and one app I saw looked at use machine learning to read privacy statements and evaluate them to give you a code of, what, red, yellow, green, what's happening on privacy. That's a privacy innovation that's being motivated by people's -- the market for more privacy or there is these apps where the message deletes itself. It doesn't stay very long. That's the purpose of that. So I think, you know, as people want more privacy, app makers will find ways to put things on the market. So...

>> NIR KSHETRI: Probably because more and more competition

and another example that Laura was giving, another good example Dropbox, I don't use Dropbox. Long ago the terms and conditions is that Dropbox will own all your data and they can do whatever they like with your data and you have to sign that thing, but more and more companies like Dropbox have come down because of the competition users like you and me have more power. And in the Dropbox example because of the complaints of user relating data owner issue and it is more friendly. More to the consumers' point of view. So consumers' complaints and consumers also have to basically work for their rights. And so -- because of the more competition and in the future more consumer friendly policies that the companies come up with. We have a couple minutes more time if you have anything more to ask.

>> I am from (Off microphone). Built one of the Smart Cities. Built (inaudible) center. Very beautiful. (Off microphone). But my point is that when -- a number of other cities look at bandwidth and see I don't want my city to become a Smarter City. (Off microphone). I hope my city becomes a Smart City if I can get that kind of smart center. (Inaudible) sorry. They said that we have run -- we have a website that's it. And we -- and I listen to your presentation. It is very nice. But many aspects that we have to see if we want to build Smart Cities. So my question is what do you think, how we can educate (inaudible) and also the citizens what Smart Cities not only technology. Smart Cities are very, very aspect we have (inaudible). Thank you.

>> NIR KSHETRI: So you would like to speak from Laura or --

>> From you actually.

>> NIR KSHETRI: Definitely Smart City is more than technology. And maybe the consumer is aware of the data, different categories of information. And how to protect that information and importance of privacy and awareness is important in the Civil Society and Government and technological like (inaudible) and engage in that type of thing.

>> (Off microphone). How to see the kind of technology (inaudible).

>> LAURA LEMIRE: You know, we've tried really hard to teach people about privacy. It is really tough. It is not I guess for a lot of people -- like I said they think about privacy statements. I think people see the value in the apps that they are using. You know, I think the younger people that grow up with these technologies I think they are becoming more savvy to how their data is being used but it is a challenge. It is a really -- it is hard to tell people how their data might be used. It is a challenge. I'm not sure if I have a great

response to that.

>> NIR KSHETRI: It is not an easy answer for that. I think our time is over. Thank you everyone for coming to the session and for your privacy session. Thank you.

(Applause.)

>> NIR KSHETRI: Person can ask Laura or me after the session. Sorry.

(Session concluded at 10:32)

***

***