FINISHED TRANSCRIPT

2013 APRIGF SEOUL

4 SEPTEMBER 2013

PRIVACY IN ASIA: BUILDING ON THE APEC PRIVACY PRINCIPLES

LECTURE ROOM 1

14:30

Services provided by:

Caption First, Inc.

P.O. Box 3066

Monument, CO 80132

1-877-825-5234

+001-719-481-9835

www.captionfirst.com

\*\*\*\*\*\*\*\*

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

\*\*\*\*\*\*\*\*

>> JIM FOSTER: Okay. I'd like to welcome you all. This is the witching hour seminar, particularly for those of you who have come from different time zones. Nothing worse than 4:30 p.m. from those who are from Tokyo or Seoul.

Thanks for coming. We are going to try to have what I hope will be a very lively and interactive session. My colleagues have been very diligent in putting together some very, very informative and useful slide presentations. I am going to be very disruptive and make them move quickly through them, but also sometimes linger because some of the slides that they have are really, really interesting.

I want to talk to you just a little bit about some of the broad questions that I'm going to be throwing out so that you can kind of get a context for what we're doing, but before I do that, I'd like my colleagues to introduce themselves. The reason I do that is because I always find as a moderator, I mangle names and backgrounds, and people are less informed or angry about who is on the panel after I've talked about them. So I will introduce myself briefly. My name is Jim Foster. I am from Japan. I work and teach at Keio University and Director of Keio International Center for Internet and Society. We have a very, very close collaborative relationship with my two colleagues from Korea University. Keio and Korea University are working very much together on privacy and security issues.

Prior to this university assignment, I spent about 25 years in the U.S. State Department doing a whole variety of different assignments and then spent a lovely 5 or 6 years working with Microsoft in Tokyo. So that's my background. I look forward to talking to you about privacy, which I think is really the topic of the day for all of us. Thank you.

Carolyn?

>> CAROLYN NGUYEN: Thank you. Good afternoon. My name is Carolyn Nguyen. I am the Director, part of the Technology Policy Group at Microsoft. As part of that organization, what we do is to look at how technology is evolving going forward and what will be the impact of that on existing policy framework. And just as technology causes some of the issues, how technology can also provide alternative approaches to policy.

My focus area is on data governance, especially in the world of big data and the incoming Internet of things. I work right at the confluence of technology, socioeconomic, and policy, and look forward to presenting and discussing with you some challenges with respect to how big data is challenging existing approaches to policy and privacy in data protection.

>> NIR KSHETRI: Good afternoon. My name is Nir Kshetri, Professor in the international business area at Bryan School of Business and Economics, University of North Carolina. I started cybersecurity for Business School students, focusing mainly on the business policy part. And one of my major research areas is cybersecurity and the international and global impact of that.

Thank you.

>> TARO KOMUKAI: Hello. Good afternoon. My name is Taro Komukai. I am an Executive Director of Internet Research, a subsidy of NTT, a telecommunication company in Japan. And my research field, main research field, is the legal issues associated with digitalization and Internet, such like secrecy of communication, privacy, or freedom of speech in the Internet or something like that.

I am looking forward to the discussion on this panel. Thank you.

>> HYUN-JOON KWON: Hi. I don't have name on the table, but my name is Hyun-joon Kwon, and I work for the Korean Internet Security Agency.

All right. My job at KISA is I am the head of the Personal Information Protection Department, and then before that position, I was -- my main job was about connectives, and so I was -- I'm very interested in the Internet Governance issues. And recently, I was one of the drafters of the cloud computing act in Korea, so I am very interested in many legal issues.

So today I am very happy to be here, and today I am going to give you some brief information about the Korean legal framework and data protection, and then maybe I'll touch a little bit about APEC's CBPR system.

>> JIM FOSTER: Thank you very much. Again, I want to thank in advance the panel. These are folks that I think are very, very deeply reflective and knowledgeable about privacy issues here in these particular markets.

Taro Komukai is actually involved in the advisory groups that are drafting now substantial privacy law for Japan, which, of course, given Japan's commercial presence in Asia and around the world, is going to influence all of us. The choices that they make are going to influence all of us.

Dr. Kwon has mentioned his role on the Cloud Computing Act. Korea, as you know, has recently passed a very comprehensive law with respect to privacy. More far reaching, I think -- and we can have a discussion about this -- than, frankly, anything else that's been done in Asia. And one of the issues that we're going to have to confront today is why hasn't there been a more expanded debate about privacy in Asia? Yeah, I know APEC and I know about Pathfinders and the principles and things like that, but the fact is that national governments have only really begun to seriously address this issue over the last couple of years, and that's fine in an era when, you know, regulation was essentially national and the Internet and the global environment was a bit of an afterthought. But the fact is that the Internet is global, and what happens elsewhere in the world, in the EU, in the United States, has a huge impact upon all of us.

I'm also delighted that Nir Kshetri is here. Nir, of course, I asked him to come specifically from the U.S. to talk about the U.S. experience. The U.S. is doing some very interesting things in the privacy field and kind of breaking the mold that the EU, quite frankly -- and I will be critical of the EU. Someone else can tangle with me on this -- has been trying to stick us all in, the cookie cutter that they are talking about, the top-down kind of approach. Nir I think can talk a bit about what the FTC is doing, how the industry in the U.S. is beginning to talk about it, what the Obama Administration is doing. Came out with very, very far-reaching set of policy proposals, very interesting.

Not incidentally, Nir is an expert with respect to the EU, so he can handle any and all questions, concerns, statements, whatever you may want to say about the EU. But actually, one thing that I'm deeply frustrated about -- and I will say it very publicly -- I spent about three or four hours today trying to do was to bring my good friend, Professor Hong Xue from Beijing, to join us. She had trouble getting a visa, so we tried to bring her in remotely, but apparently we don't have the technical capability to do that. So I'll put that right on the record.

But fortunately, we have Nir here because Nir also is an expert on China. So you kind of say China and privacy, isn't that a bit of an oxymoron? How do those two go together? The fact is China has passed a rather comprehensive privacy law and is continuing to develop aspects of it. And just like economics and politics are separated in a global sense, they're very much separated in the privacy world. Chinese consumers expect that their privacy is going to be respected. They expect that their transactions will not be misused by the companies that they choose to do business with. And so in many ways, they are just like all of us else around the world in the area of consumer and commercial transactions.

And if you think -- and this is one thing that I'm going to be throwing out here -- if you are talking about privacy, are we talking about consumer rights? Are we talking about privacy in a business situation where there needs to be a balance between the interests of the companies that may be providing certain services, in return for a currency, which is privacy, which enables -- in facts, drives -- a lot of those services? So a commercial kind of perspective on privacy that certainly exists, and I would argue we need to watch carefully because it could be defined by China here in Asia.

And then, of course, the broader kind of political, human rights, fundamental sense of person. And certainly the EU is -- takes that as a fundamental aspect of their approach to privacy. There are certain incredibly important aspects of that. There also are issues that are very, very complex. So I hope that we can address them.

And I think that the key for this -- and this is why I'm delighted that Carolyn is on the program -- is that I think we've gotten too hung up on the regulation of privacy. And we've been trying to come up with rules to protect without asking ourselves at the end of the day what are we protecting? I mean, and when you try to ask that question, who should you ask? We should ask the people who are actually being -- who actually have privacy, consumers. So what is the consumer perspective on it?

Everybody kind of has a sense well they know what the consumer perspective is. Carolyn is kind of an empiricist. She actually asks the questions and tries to understand what consumers want, and what she finds -- and she'll talk in more detail about it -- is consumers are incredibly diverse and also, to some extent, incredibly sophisticated in the way that they think and use privacy. Because how many times have you clicked on something and said, you know, I really am happy to share this with this company because I see something tangible coming to me? So there's a transactional character to privacy as well as these other aspects to it.

So we're going to kind of move through today just to give you a quick overview of where we're going to go. Taro and Hyun-joon have provided some excellent background on what is going on in Japan and Korea, and Japan is grappling with the law. Hyun-joon will tell us a little bit about how Korea got to where they are. I think it's tremendously significant for the broader debate here in Asia.

Nir, I think, is going to offer us some thoughts and some slides with respect to the U.S. experience. Perfect. Perfect. So as I said, we're going to have a lot of fun, but we're going to move quickly because I want to pull out some ideas from you.

And then we're going to have Carolyn kind of address that consumer perspective and how that comes together.

And so I do want you, as you are kind of thinking through these things, to recognize that if you look around the world -- and those of you who are suffering from jetlag will understand this in a second -- that there's really only going to be three economies in the Internet world: North and South America; Europe, Middle East, Africa; and Asia from India to Japan. And that's called time zones. And you certainly don't want to have an Internet relationship with somebody in the wrong time zone, so naturally, economic activity is going to be flowing from that. and in that particular context, then, we know where the U.S. is beginning to move on privacy. We know what kind much rules are going to pertain in the EU zone. What happens here to Asia? Is Asia going to be derivative of developments there, or is Asia going to, given its diversity, given its contrasting levels of economic development, and given the ingenuity of all the people here in the room, is it going to strike out a different course and hopefully a better course?

We have the two leading countries here who are beginning to place their bets. China, of course, is placing some bets as well. So those are kind of bellwethers. If you want to know where we are going to be on privacy in five years, I think you are going to hear the trends spoken today.

So I will shut up. My big fault as a moderator is I talk too much. But let me turn it over quickly to taro. Taro, Hyun-joon, ten minutes or so, ten minutes each. Do your best. If you go a little bit over, look at me and I will look at you. Okay? Thank you.

>> TARO KOMUKAI: Okay. First of all, I would like to make an explanation about the scheme of regulation about personal data protection in Japan. It is a little bit complicated, but I will try it as brief as possible. Okay?

Let's go to the page 3, please. Oh, okay. I will manage. I didn't realise it. Okay.

This is a framework for personal data protection in Japan. We have a basic law about personal data protection. The Personal Data Protection Law of 2003. This law provides how to protect personal data in Japan and obligations on the enterprises which process personal data.

As for the public sector, there are two other acts, the act on the protection of personal administration, held by administrative organisations, and the act of administrative agencies.

And there are 37 guidelines for each industry based on Article 8 of the Personal Data Protection Law and more than 2,000 ordinances by local governments and municipalities. These guidelines and local laws include different regulations. It is a very complicated regulatory system.

Okay. This slide shows the outline of the obligations for business entities handling personal data provided by the Personal Data Protection Law. Entities handle data of less than 5,000 individuals are exempt much these obligations, but the exemption for small business is criticized as unreasonable or could be a loophole of regulation, especially by you. I think it may be abolished in next reform.

Okay. I will explain the outline of the obligation. The entity must describe as specifically as possible the purpose of using personal information and notify or make public announcement of the purpose of use. Unjust method of collecting is prohibited. Unjust means deceit or other unfair or fraudulent way. The entity shall not exceed the scope of the purpose of use unless it obtains the prior consent of the person. The entity shall not transfer personal data to any third party without the prior consent of the person. But this prohibition is exempted when the prior opt-out option is provided. Joint use is also allowed when the purpose and joint member are announced in advance.

As for security, there are the provisions that require data integrity and security control. In addition, the entity shall appropriately supervise its employees and contractors. The participation of the person is provided in the provisions for disclosure, correction, and suspending of utilization.

This is a slide for describing the enforcement by competent Minister. We don't have any privacy Commissioner or commission in Japan. A competent Minister supervises the entities.

Failure to comply with the Act may result in other administrative penalties. The competent Minister may issue recommendation or an order. If the entity does not comply with the order, the person in breach of such order could be accused as a criminal offense. But there has been no case in which the entity was held criminally responsible.

I think Japanese data protection scheme has two critical problems. One is lack of the privacy commissioner or some other type of authority which is responsible for the rulemaking and enforcement. The other is that there is no provision to assure the appropriate purpose of use. The Personal Data Protection Law in Japan requires entities only to make a public announcement of the purpose of use. It doesn't require to obtain the consent of the person, like the regulation in EU or Korea. And there is no provision which prohibits the deceitful action in use of personal data like the regulation in the U.S.

Therefore, even if many people think a particular purpose of use is uncomfortable, the use cannot be restricted for the reason that the purpose of the use is not appropriate.

Okay. Let's go into recent topics. Now, in recent years, the government in Japan has been discussed on their issue of privacy online or big date. There have been some study groups and working groups which discussed the protection and privacy online for new situations such like big data. First one on the slide is a report of the Study Group for Securing of Personal Data at the MCAC, Minister of Community Affairs and Communications.

Second one is output of the discussion focused on the issue associated with smartphones.

And the last one is the working group at METI, Ministry of Economy, Trade, and Industry. I was a member of this working group. We focused on providing sufficient information to consumers, not in a reluctant way. It will be important to make the matters to be described and styles of expression better to be user friendly.

The way of identification is also a topic on this discussion. MICC study group proposed requirement of the identification to transfer the data as no personal data. It is something like standard by FTC. It stated that, one, the company must take reasonable measure to ensure that data is identified. Two, a company must publicly commit to maintain and use the data in an identified fashion and not attempt to reidentify the data. Three, if company makes such identified data available to other companies, it should contractually prohibit such entities from attempting to reidentify the data and monitor that compliance with the provisions that should be made.

Such recommendations made by government authority has two meanings, I think. First, it could be a guideline for enforcement by the authority. If the guideline says the entity can use personal information in a particular way, the usage won't be subject of enforcement or prohibition. Second meaning is that the authority is merely recommending something like a privacy advocate. I think the recommendations and guidelines by Japanese government are not guidelines for enforcement because they rarely make enforcement on personal data treatment. But the enterprises in Japan are well complying the guidelines by government authorities. I don't know why.

Comparing with FTC, recommendation by FTC goes hand in hand with the enforcement. As for the identification, if a company does take steps to reidentify the data which it says it is identified, it could be illegal under Section 5 of the FTC act.

During this discussion, I think that prior consent, no tracking data, no tracking data possibilities are covered, but there is no discussion on the right to be forgotten, which is discussed -- which is now discussed in the EU. I think the right to be forgotten is not fully a concept still now.

Okay. I would like to introduce the Social Security and text numbers in Japan.

A Social Security and text number system is going to be reduce introduced in Japan. There has been strong resistance to introduce a number system in Japan, but it got agreement that it is necessary to introduce the needs of a society of low birthrate and aging population.

I also attended the working group to protect privacy about the number system. The bill for the number system was enacted on May 13 this year. An independent supervisory authority will be established in 2014. This would be the first independent authority of personal data protection in Japan.

Recently, Japanese government released a policy to conduct the regulation reform to promote the use of personal data. It says the Japanese government will immediately establish new study group under the IT strategy headquarters and start the discussion to clarify the rule about making the best use of personal data with consideration for privacy and data protection, reform of data protection guidelines, standardization of the way to obtain users' consent. The study group will also make reform policy and roadmap including establishing of the third party authority and new means of enforcement within this year. The study group started discussion the day before yesterday, this Monday.

Okay. I will make -- may I make a short remark about the issues to be discussed? Three minutes. Okay. Okay.

I would like to talk about the international harmonizations. Japanese government submitted the application for attending the CBPR of APEC in June. I understand the CBPR scheme is designed to assure the data protection in cross-border transfer by the combination of certification and enforcement. I think it is one of the approaches to interoperability.

As for the international -- Oh, I am sorry. CBPL APEC, yeah, I am sorry. I missed the pronunciation.

As for international harmonization, the OECD 1980 guidelines are going to be revised. I hear that the final version will be officially released in next week or something like that. On the discussion of that, the approaches on the side are referred as important approaches.

I think that multiple approach will be necessary for the moment to proceed with interoperability of personal data in global level. And I would like to make a brief comment about the U.S. and the EU and Japan, EU and the U.S. In EU, data protection is considered to be directly required from fundamental human right of privacy, my understanding. And I think what they think essential is to reflect the will of the person on the processing of personal data. Obtaining consent from the person or providing opt-in option will be important there. On the other hand, the U.S. regulation on consumer privacy is based on the concept of fair competition with customers, consumers choice. The concept will likely require the opt-out option for the well-informed consumers. If the opt-out or information for the users are not sufficient, it could be a subject for enforcement.

EU and the U.S. have different basic concepts for the personal data protection, but when it goes to the actual requirement in each case, the difference could be small because both approaches require respect for the individuals. The approach in the U.S. is very unique, and few countries take the same one. But I think it will be possible to go well with the requirement of the U.S. regulation for many countries.

As for EU regulations, it will depend on the regulation which will be made in the near future, now under revisions. If the requirement for the consent comes to be too strict or strong, many countries might be unable to meet the requirement.

I am sorry, I exceeded my time. That was my opening presentation. Thank you.

>> JIM FOSTER: Hyun-joon, please. You are going to talk about Korea but also offer some comments on the APEC framework.

>> HYUN-JOON KWON: Okay. I cannot see my presentation here. It's very odd here.

Okay. My presentation is about -- okay. My presentation is about PI, personal information, protection, about the legal framework in Korea, and also I will touch a bit about enforcement in APEC, the CBPR, of course, with privacy rules in Korea.

I want to talk about the expansion of the concept of personal information. Basically, we have known personal information, real names, Social Security number, and then also we think the bio information, fingerprints and those things, will be the personal information. Also, recently these days, we are using the LBS, local information-based services, so we are using location information.

Also in the Internet, you know, you are shopping or you are searching, so your behavior information is very important for -- to optimize their advertisement. So that's the changes of the concept of personal information.

So also most of the personal information flows mostly on the Internet, not offline or more than offline. So because of many reasons of this, so you can read it. I will skip this one.

This is the big picture about our legal framework in Korea about personal information protection. We have a general law here, Personal Information Protection Act. This applies in many areas, but if there are some special laws, then that law will apply first, and then.

So we can -- I just divided the personal information, like personal information, online commerce. In that case, we apply this law. It's a long name, act on promotion of information and communication network utilization and information protection, et cetera.

Then also the personal information, location information, in that case, we apply the Location Information Act. This is act on the protection of location information. Also, for the credit and financial information, this law applies, and then health information, there are many laws. So these laws apply to this information. Also, student information, student, grade records, those things.

So here I am telling you in Korea, there are many laws regarding personal information, so they are very complicated, but anyway, we have one basic law, and then we have very special laws on each special area.

So it's very hard to manage the business here. This is about our government structure. So you saw the Personal Information Protection Act, the basic law, which is -- that is administered by the Ministry of Security and Public Administration. So this department is coordinating the whole area of privacy and personal information protection. And the reason I circled with a blue color here is because this session is a little bit related to the APEC CBPR. The CBPR usually applies on electronic commerce, so this is the -- I'm interested in personal information online comments or services, so this one -- the act applies here. That act is administered by the KCC department. So if any countries want to talk about the APEC CBPR in the -- on the electronic commerce, maybe you can talk to this Korea communication commission is the right department.

And then also the credit information, you can talk to the Financial Service Commission. And if you want to talk about health information, the Ministry of Health & Welfare, then student information, maybe you can talk to Ministry of Education. That's our structure of government.

So there are many laws, but I chose this act because it applied to all the personal information in the online commercial section. So according to this act, there's some definition of personal information here. In Korea, we usually use this. Personal information is about the information of individual life. Also, personal information is about identifying a specific person. Also, personal information includes the information that does not make it possible to identify by itself, but it enables to identify a person easily if combined with other information. For example, there is white hair in this room, white hair, and then, you know, blue shirts. Or maybe taller than two meters. If there's one person, if we combine those information, and if -- yeah. Separately, that's not personal information, but if we can combine it and identify someone, we call that personal information.

This is the picture like that.

In the Network Act, there are many chapters because this is basic law about the Internet activities, and Chapter 4 is about personal information. So if you want to -- interested in the Korean law and personal information in online commerce, maybe you can look up this part.

Also, Chapter 8, international cooperation, there is specific information about transborder flows of personal information. So I will talk in detail.

>> JIM FOSTER: Dr. Kwon, can I interrupt a second just as a question? Why is it this authority was given to the KCC instead of creating a privacy commission?

>> HYUN-JOON KWON: Actually, our law is different because in the basic law, there is -- Oh, about the committee. There is a law. According to this Act, there is a mandate of the Committee. So in that, according to the Act, maybe the Congress and all the people at the time they made such a framework of our government, but anyway, according to this Act, our Personal Information Protection Committee does not have some kind of administering power. They will be the coordinator. If there is some kind of legal interpretation conflict between two departments, and then he will advise, and then maybe he can show the opinions to departments. So this committee has its role, but it does not cover one area or it doesn't have -- have like direct act or it doesn't have any enforcement activities.

>> JIM FOSTER: The KCC has enforcement authority, just like the FCC?

>> HYUN-JOON KWON: Only in Internet -- profit activities on the Internet.

>> JIM FOSTER: The reason I ask that, because as taro knows, that is a key question that's now being discussed in Japan is -- because I think his presentation outlined how there's all kinds of guidelines in Japan, and actually, one of the reasons that there's such great compliance in Japan with those guidelines is nobody is sure what's legal and what's illegal. It's a very, very confusing environment for businesses, creates a lot of uncertainty, stifles innovation. And so I wonder is the KCC and the FTC model -- it's certainly different than what we find in Europe where they have privacy commissions and commissioners. And actually, other parts of Asia. I believe Singapore also has a privacy commission.

>> HYUN-JOON KWON: Yeah, that's right.

>> JIM FOSTER: Was there a discussion along those lines? Because it seems to me that the KCC would take a more balanced approach because they're also responsible for promoting president Internet as well as regulating the Internet.

>> HYUN-JOON KWON: Okay. At the time of enactment of Personal Information Protection Act, there was a very serious discussion about powers of personal information committee because we studied a lot of the EU model, the commission model, and then also we studied many countries, Japan, U.S., and many countries' models, but I cannot talk about the details, but anyway, the conclusion was the commission will be the coordinator, and all the departments -- I think to leave the privacy policy and all the activities to departments more efficient, maybe. So that's why I think they made this act like that.

Also, another question was about -- what was it?

>> JIM FOSTER: I think you covered the questions. I just wanted -- you had made a comparison, and you thought that the KCC had the enforcement authority to make these decisions, even though there is a coordinating body to be sure that all the different ministries are evaluating their programs in a consistent way.

>> HYUN-JOON KWON: Also, the departments, as you said, they are very interested about balancing issues. Utilization. We have also they need to regulate. So they were always having some -- we have very serious discussions about. Because personal information will be, you know, the engine of the future industries because this will be should it be utilized for more -- because in the future, society will be more human centered, you know, industry will become the future engine of the future society.

So also, private personal information is very vulnerable, you know, when we use those services and when we use personal information in many areas, and then maybe the personal information will be misused also.

So that's always when we, you know, have a discussion about policymaking, utilization is a very big issue.

>> JIM FOSTER: I took some of your time, but I am only going to give you three more minutes.

>> HYUN-JOON KWON: Okay. Okay. This is the -- this is our definition. And this is recent change in our Internet Act, so if you are interested, please read it because some of it is very interesting.

Because this session is a little bit about related to the APEC CBPR, so I am just going to show you some brief information about Article 63 of this Network Act. This one is about the protection of personal information. The company should execute an international contract in violation of this Act -- that's the mandate. Also, if the company intends to transfer personal information, they need to obtain the consent of the user. Also, the company should not find all the following events, so the transferring, the state to which the information is going, the date and time, and the method. Also, the purpose of the use and the period of time of possession and use of the personal information, that's the minor thing.

The next one will be the hard one for the company. If you want to transfer the user's personal information to abroad, you should take protective measures as prescribed by Presidential decree. The Presidential decree has many requirements, especially, you know, in the decree there is Article 15, and this one is so many things, Chief Privacy Officer and PI process information, sometimes access control of the personal database system and file protection. This one is also a very hard one.

Separation of Internet from personal information database. If there is one computer processing personal information database, it should be separate from the Internet.

And then those are the things. Also, there are more details,. If you want details, there is a Ministry ordinance of KCC, and then there are hundreds of requirements. I know. So that's the very hard one.

And then I don't think I have much time, but the APEC CBPR, I will tell you about enforcement to APEC CBPR.

The CBPR is setting up the codes or conduct that should be backed up by the government. And also there is one more thing about the CBPR does not replace or change the domestic laws. Also, the way there is applicable privacy protection comment in the economy, the CBPR is the solution to provide a minimum level of protection. That's the main idea of CBPR.

So KCC right now is taking the -- we are considering participating in CBPR, and then maybe in this year, maybe we have some discussions about other countries.

Also, the -- I'm mostly involved in some agreement discussions. There is some electronic commerce structure. Some countries don't like it, but always transfer data flow of personal information. Some countries -- I cannot mention the name of the countries -- but some of them, they do not like it.

So this is our -- we are considering that one, so also we need time to review the experts' opinion about these issues.

I think that's all for my presentation. Thank you.

>> JIM FOSTER: Okay. Well, thank you very much. Dr. Kwon, just a fantastic presentation. A lot of information there. The slides are going to be published, and you should take a very, very careful look at them.

I think just a little commercial promotion. Our university, Keio University, is working with Korea University on talking about privacy. And we are working hard to develop a dialogue between Japan and Korea. One, because I mean, Korea has really gone far down the road on a number of things, and actually, has wrestled with a lot of the questions that taro and his people are talking about right now in Japan.

Also, quite frankly, whatever these two guys decide is going to have a huge impact, I think, upon the rest of us in Asia. So thank you very much.

I am now going to turn to Nir. He is only going to cover the United States, the EU, and China in a few minutes. In a few minutes. Because I really want to get to Carolyn in the sense that, you know, we're talking a lot about what the governments are doing, and we are making a lot of assumptions about privacy and how you protect privacy and how you create an administrative framework that allows you to regulate it. But at the end of the day, you have to ask yourself what in the hell are we regulating, and why are we regulating it? And I think Carolyn is going to get us back to some of those, you know, more basic kind of questions and look at it from an empirical perspective. Not what we think about privacy necessarily as academics or practitioners, but what actually people who are transacting these things -- when you put on your consumer hat, I bet you behave a lot differently than you do in meetings like this. I know I do. I say well, I know they might misuse this, but heck, I really want to see that particular piece of content, or whatever.

>> NIR KSHETRI: Okay. In this one, I will be emphasizing mainly on three points. First one is the U.S. approach to data privacy protection. Then the second point is the comparison between the EU model and the U.S. model and the Chinese model in terms of data privacy protection. And the third thing is that in addition to the government, there are a lot of other actors, like the special interest groups, trade associations, professional associations, and international organisations. What is their role in the debate about privacy protection? Those are three points.

First thing is the U.S. model, very briefly. The U.S. approach to privacy protection basically -- which is different from the European Union approach -- is to mainly rely on self-regulation. But at the same time, U.S. has some of the very national security related or some industries which the U.S. specifically requires very high level of control, high level of regulation in the sectors.

One example is the Sarbanes-Oxley Act, which was enacted in 2002, and that basically requires all the financial components, like bank and other financial institutions, and their information technology control mechanisms, they have to make sure that the data are accurate and they are protected from unauthorized changes, that is in the financial sector.

And if you look at the healthcare-related data, there is the HIPAA Act, which was enacted in 1996, and the purpose of that is to maintain physical and administrative security measures, basically, the privacy, integrity, and availability of personal data. And those who fail to comply, I think the number recently increased, that is 1.5 million fine. It has increased. And the violators, if they are repeat violators, might face up to a ten-year prison sentence.

I will come back later a little bit more about the U.S. approach in comparison to European Union in China.

In addition to these, one of the important features, so one of the discussions are in the context of the cloud computing, evolution of cloud computing, and also the U.S. has the Federal Information Security Act, and basically, which is different from EU. EU allows personal data transfer only to nine countries. And for example, the European Union doesn't consider Korea, Japan, having adequate level of data protection, and only nine economies that European Union has basically recognized to where personal data of European citizens can be transferred to include Switzerland, Argentina, Canada, a couple small economies.

And compared to that, U.S. really doesn't care about transferring healthcare data to other countries or financial data to other countries, as long as they are protected. And the only requirement in the U.S. is that if there is the federal information, federal information, cloud providers, like Google or amazon.com or any cloud providers cannot take the federal government information outside the U.S. companies. They have specific cloud information specifically developed for U.S. federal government agencies.

Now, these are -- one of my forthcoming papers in security and privacy. So I have compared these models in terms of the salient features of China, EU, and the U.S., and what are some of the key driving factors and what from the sides of providers and IT users.

The first thing is in China, China's information technological development, since long ago, maybe from the 1990s, has to balance economic modernization because the Chinese communist party derives a lot of -- from the economic growth, and they don't really care much about the -- thing. At the same time, the main emphasis has been to maintain stability of political control, and emphasis is maintaining healthy and harmonious environment. That is what government emphasizes, key driving factor in China.

Which is different from the EU. The EU, irrespective of any type of information, there should be very strict enforcement of privacy rights through legislation, and the European Union, that approach can be basically attributed to if you go back to the second world war period of time, and after that, following that, a lot of these communist governments in many of the European Union countries, Hitler and many of the communist governments, they basically used personal information, abused personal information, and so Europeans are very conscious of government using that information. That is the main driving factor in the European Union.

And if the look at the U.S., the U.S. approach is to encourage marketing and mainly utilize self-regulation, and the government doesn't really enforce a lot except for those things.

And the IT providers, okay, the main complaint all these foreign companies, or even the Chinese companies, have about the Chinese regulation is that there is no specificity about understanding and complaints. For example, which department is responsible for enforcing that law? And there have been many laws. Privacy protection in China, even the Chinese Constitution in 1982, Article 40, has specific thing about so no one business, individuals, or even government agencies cannot infringe on a personal privacy. But there is really no definition of what exactly privacy is, and the definition of privacy in China came only in 2012. But there is regulation, and they have enacted a lot of things, but there are a lot of these complications and specificity which eventually will enforce that and will supervise, and also another problem is if the police or law enforcement people are doing some type of inspection and there might be equipment loss and all those things, so there is no one -- no one really is responsible for that in China.

And if you look at the European Union countries, there is the strict regulation and lack of economies of scale. European Union has 27, actually, 28 economies right now, and although they have these 28 economies broadly follow the same, the enforcement varies widely. If you look at enforcement in France, there might be violation of privacy protection, the fine is up to 150,000 Europe, if you go to Spain, maybe 300,000 euro. So a lot of those irregularities, variation across those European Union countries.

And some of the newly -- like Bulgaria, these countries do not have same level of resources like Germany or France to enforce data privacy protection laws.

In the context of the U.S., the main concern has been simply many of the European Union-based consumers and activists and recently high-level policymakers like the European Union, European Commission, even the German Interior Minister following the June 2013 PRISM surveillance program, they have been complaining about the cloud service providers because one problem in the European Union countries is they do not have very high-level cloud providers at the level of Google or Amazon or Microsoft, those U.S. companies. And these U.S. cloud providers have to make some adaptation to function in the European Union market, but still, they are good. They are better than many of the European Union cloud providers. But many of these European activists and policymakers are complaining about these U.S. cloud providers because the U.S. has the Patriot Act and also the foreign intelligence amendment Act, something like that. Surveillance Amendment Act. Basically, Microsoft Managing Director in UK a couple years back said that even the UK cloud providers' data might be basically -- they fall under those acts. And that basically increased the distrust among the European Union activists and consumers and policymakers for the U.S.-based cloud providers.

So the main concern for -- actually, for the U.S., it is more concern from the European Union. I don't know that situation in Japan, if they trust or do not trust the European Union, but I have read a lot about the concern in the European Union countries.

And looking at the users, what is the effect on the users? And if you look at China, there are not a lot of availability of services, like Google is not available in China, and if anyone wants to use Google, Google redirects that to the Hong Kong data center. And also Google has data centers in Singapore and Hong Kong and also recently bought land in Taiwan. So the Chinese consumers that want to access the cloud services or any information technology services provided by these foreign companies, they basically have to get that from outside. And there is very strong firewall protection and that either services are available, I can look at Google or dropbox, these are not available. Or if they are, then it takes a lot of time to download that. So this is this has a lot of concern in ITU.

So if you look at the European Union countries, high level of privacy there. The European Union users enjoy high level of privacy. But the problem is cloud and other types of services are not available in UE countries compared to the U.S. And also, monitoring and misuse of information in the U.S. Just coming back to this point, they are saying this cloud market will be about $800 million, many companies are estimating by 2016, and U.S. accounts for -- so one problem is that the online advertising is not working very well in European Union because of the concern there is lack of information about consumers. There is a lack of polity of information about consumers. And there is a lot of cost to maintain that information. So for example, the European Union has right to the clause which requires if you request Google or any company to delete your information, they must do that, which is not the case in the U.S. So that basically is a concern in European Union countries.

My final slide is that so government is playing an important role, and in addition to government, there are these special interest group nongovernment organizations and trade association, professional association, even the information technology vendors, they have been playing a very important role. In the U.S., they are specifically asking the Department of Homeland Security to stop whatever the national identity system -- this is in the U.S. -- and Europe, the European telecommunications network operator organization that was lobbying for international privacy standard because the European standard is too strict, and that is basically becoming a hindrance for the development of cloud. And all of these companies, Oracle, Cisco, SAP, Apple, all of these companies are lobbying the government in EU.

Also a little example of India and China. In India, special interest group or trade association, the national association for software and service companies, which represents all the software and service companies more than I think 1300 members or 1300 companies currently, and more than 200 are global companies from Japan, China, U.S., or many companies. And in India, many people are using Internet for the first time. (Speaker off mic). They don't really care a lot about privacy. But this NASSCOM has been working very hard, taking a lot of initiatives to develop the data privacy protection in India. The goal is to have the same level as the European Union or the U.S., so because of the growing outsourcing industry, estimated as kind of $108 billion every year, but the European Union has concern about the low level of protection in that.

So I think my time is over. Thank you very much.

>> JIM FOSTER: I think you can see there's just enormous complexity and substance to this debate. And I think as you can see what's happening in China, it bears very, very close watching, as well as you can see the EU probably has the gold standard for privacy protection, but what is the cost of that? And the cost is in slow growth, it's in lack of competition, innovation, and now, of course, you are finding companies actually relocating out of Europe because they find the standards and criteria to be too onerous.

So I think it's a nice way to tee up Carolyn's thing by asking the question: What is it that people really want?

>> CAROLYN NGUYEN: Thank you. Thank you, Jim, for teeing that up.

So my role here is really to look at, you know, so a lot of the regulations and policies that we are looking at here is essentially based -- even the APEC framework, et cetera, is really based on the OECD principles, and in the U.S., the FIPs principles. And when you start to look at that, it's all based on consent, which assumes that the user is giving informed consent. So we know there's been a tremendous amount of research that says that's really not the case. Most users automatically just click "I accept" and take on whatever.

So the question is that, you know, a lot of these regulations are purported to protect the user, but at the end of the day, is this what the users really want? And this is a really, really important question to look at because there's an emerging data-driven economy where I think it's been alluded to by others that there's more and more data going to be used. Now, in a data-driven economy, value comes with enabling data to flow. And you see that -- and that value really comes from enabling the insights that would be derived from commingled data sets. And essentially, if you are going to create a sustainable data ecosystem, there really needs to be a balance between innovation and economic growth and consumer protection. That tension is exactly what you see in a different approach between the U.S. and the EU, with the U.S. more oriented, as Nir mentioned, towards market growth, and the EU more towards consumer protection.

Now, what happens is that big data poses much further challenges to this issue of balancing. That's what I want to spend a little bit of time exploring.

Before we start, I am sure you are all aware of the numbers already, but let's just kind of throw a few numbers out there so you can get a magnitude of the issue with respect to big data.

Between 2010 and 12, the number of devices surpasses the number of people. So 9 billion devices versus about 7 billion people. By 2020, that number is expected to reach 50 billion devices. So when you start to think about that, what you start to see is that the majority of data generated will be generated through machines-to-machine transaction. And when you contrast that against a model which is based on consent, you start to see some of these issues. Okay?

So with that, I'm going to go to the next slide. So when we start to look at that and that simple statistics, so the privacy landscape is evolving. What the model is today -- and this is essentially true regardless if it's APEC, the EU, and in some cases the U.S. model -- the assumption is that the user is actively participating in the transaction where data is collected. This is the basic premise behind consent.

Going forward, data is going to be passively obtained. Remember, there's 50 billion devices versus let's say even if the population is growing much, much less, maybe about a fifth of those number of devices. So the user is not going to be aware of many data transactions.

The second thing is today, what is considered personal data is predetermined. In fact, the majority of regulations takes a stand that says personal data is defined as this, so location data is defined as personal, and start to put severe restrictions on what can be done with that personal data.

Now, going forward, in the area of big data -- and again, when you start to ask any user and I think when you start to consider users' mental models -- the notion of personal is very much dependent on the context it's used and subject to cultural and social norms. How many of us have said that financial information is personal and won't really -- and would be really nervous to input personal credit card information online. Just let's say take a number five years ago versus now. So what's considered personal is changing, and it's subject to cultural norms. This is one of the issues when you start to say, okay, is location information personal information or not? Well, it's a personal decision.

So in the U.S., the FTC starts to take some of this into consideration as well as the White House in its consumer bill of rights because they start to talk about context aware data usage.

Today -- and as a basic issue in terms of the OECD principles is collection -- you know, purpose limitation. Data is collected for a specified use. But when we talk about data in a data-driven economy, that's clearly not going to be the case. So I think there's some questions. I think there was a comment earlier on the OECD principles are going through a revision, but they are not going to revise it. What they'll do instead is the OECD will establish a new project that's based on big data. They'll revise the OECD principles in the context of big data, and that's a project that's starting essentially this year.

And today, again, the principle says user consent is required, but we all know, as I mentioned before, that users are not empowered. In the big data world -- and for those of you looking at it, the Internet of things -- because that was mentioned this morning -- it's a decentralized data ecosystem. In other words, no one is really in charge of that ecosystem, and there isn't really a single ownership of data. And so it makes user consent incredibly impractical.

The current policy focuses on minimizing all personal risk. Outside of the U.S., it's tilted more towards user protection, and we all know, I think, as Jim mentioned, that overly conservative approach will limit benefits as well as innovation and potential growth.

So what does that mean? What happens is so coupled -- here's the issue. Coupled with that shifting privacy landscape is the fact that today there's a crisis of trust in data use. In today's world, because the service providers are oriented towards -- tend to have quite a bit more personal data, there isn't trust from the consumer or the user. So if you are going to build out a sustainable data ecosystem, there really needs to be quite a bit more focus on trustworthy data practices as far as the user is concerned.

So with respect to that, the World Economic Forum started a project called Rethinking Personal Data. It's in its third year now, which really looks at approaches to personal data to engender the trustworthiness in the data ecosystem. So a little bit different; right? Because when you start to look at existing policy and regulations, it's designed very much top-down and more bureaucratic manner as opposed to really taking the user's perspective into consideration. And in looking at that, the World Economic Forum carried out global -- conversations globally. Here, what I put up here are some of the conclusions that they came to as a part of that global conversations with policymakers, consumers, civil societies, and industry.

So given the world of big data, it's very much shown that a new approach to personal data is needed, and there is a need to shift the conversation to data use. Today, when you start to look at consent, that is done and given at the point of data collection, where use is clear. At the end of the day -- and I will go a little bit out on a limb and say at the end of the day, what you just care about is what use is the data or any data about them is being put to use on as opposed to what are all the information that are out there about me. So we've conducted some major research on this to prove that.

And so today -- so what that means is if you're going to build out a user-centered data ecosystem, there needs to be new ways to engage the user. Today when you start to look at the majority of principles, that talks about transparency, which is translated into let's put all the information out there as opposed to how do you meaningfully engage the user in interactions? And so this is one area which -- where context is really, really important.

Technology can be a part of the solution. Thus far, a lot of the approaches look at designing policy separately and almost in a bureaucratic manner, separate from technology, instead of looking at how technology can help. So we explore some of those -- some of that within the World Economic Forum project. And then set about to try to build out a usage-based contextual model. Essentially, the notion is how can we work together to build up an evidence base while at the same time researching policy approaches that will be fit for this world.

So what I've put down below is that at the end of the day, any sustainable policy framework needs to take into consideration the interest of the service provider for sure, but absolutely the users and the regulators, and it really needs to be context aware. Sustainable because that's the only way that it can work. So with this as a little bit of background, what we did was embarked on global research. It's a multi-phased research that is done at qualitative as well as quantitative. We did it in eight countries. And the countries that were chosen kind of outlined a boundary of the various different approaches to data protection regulations. And what we found, in a nutshell, is that user attitudes regarding personal data is quite a bit more nuanced and context dependent. It's not binary at all. And some of the elements that users take into consideration when looking at whether data can be used or not include the type of data. That's well known. There's been a fair amount of work out there that says, you know, what are users' sensitivity to medical versus financial information? The type of entity that they are interacting with. Is it a service provider? Is it a government? Is their employer? What level of trust do they have in service provider?

Initially, we thought this was a trump card, in other words, if you had trust, the user would do anything. But it's not. It's just another factor. It's a necessary but not sufficient condition. Okay?

And the collection method, how is the data collected? Passively, actively? And this was really hugely surprising to us that when data was passively collected, users were still okay with it, especially users in China. And to our surprise, Germany. Yes. And India. What kind of device are they using? Are they on a mobile device? Are they on a desktop, are there on a tablet? How is the data being used? Is it being used according to the way that I consented to, or is it being used autonomously, in other words, automatically through something? And what is the user getting out of it? This is the part that actually gets -- doesn't get addressed at all in any of the existing regulations. So in fact, in our conversation with the OECD, we proposed that when they start to look at the OECD principles as it relates to big data, that they need to really take this into consideration because it is a part of that consideration.

So lots more data on this as well as what are the cultural and social norms and how does this vary across country? Just so you feel a little bit better, China and the countries in Asia are much more oriented to what's user data for community benefits in the developed world. In the western world, people are more willing to share data that results in personal benefits. So we kind of said, okay, the west is just too geocentric.

So in a nutshell -- which is a summary, big data raises really a need for user-based approach to data governance. It's essentially a call to say in this coming world, there needs to really be new thinking about some of these issues that are being posed to the basic underlying principles of which many of the existing regulations are based on. Because this is an academic environment, I just want to -- you know, I think we need to do research both in parallel, both in terms of technology, technology in quotes, because -- as well as policy when we start to look at some of this because it is really, really clear that new policies are needed. And then let's work together to develop an evidence base to inform policymaking.

There is a conversation we started in the U.S., in Europe, as well as here in Asia, about the new research that are needed and to really focus on what users are thinking, what are their mental attitudes, how do they look at the use of their personal data. The issue of who represents users in regulations is an interesting one because most people will say civil society and consumer organizations, whereas the reality is the data we have founds and data from many research organizations doesn't necessarily echo that.

So that's it. Thank you very much.

>> JIM FOSTER: You can clap.

(Applause)

Really good. You know, I saved the best for last, and not in the sense that it diminishes the other presentations, but I was delighted that Carolyn was ready to come out from Redmond and talk to us because it kind of stands everything on our head; doesn't it? It doesn't change your thinking, but it changes your perspective on what you thought you knew. And when it's also linked to this advent of big data, where stuff is being collected passively -- I mean, how many of us think when you are going through the toll booth at the highway that you need to sign a consent form for the traffic authorities but also a whole range of authorities to use those images of you as you go through? A lot of information in those pictures. I mean, your car, your -- I mean, there's a lot.

And it really does raise the concern as well as we look at, for example, what is going on in Korea and Japan and in the United States and in Europe with respect to these rapidly emerging and evolving and sometimes very conflicting data protection schemes that do we really know what we're regulating?

Because one of the sad facts about government -- and I spent a lot of time in government -- is it takes a long time for a government to make a set of decisions. Very complicated. A lot of important interests need to be balanced. And you know what? Once they've made a decision, they don't like to go back. They don't like to reopen it. And so you're left, often, with contending with the legacy of policy decisions that were based on assumptions in technology. Japan is actually a classic example. They have a personal information law from I think 2003. And they have been regulating privacy now for ten years now based on a framework that even at the time was considerably behind where most countries were in terms of their legal definitions and administration of personal information.

And so I think we really need to -- as we're also talking about these issues also take a hard look at the mechanisms that we use, both internally and now in a broader regional and global environment to make these kinds of decisions. Because we can't wait. I think as Carolyn side, we are going to be overwhelmed by the Internet of things within a very brief period of time, and what is going to happen with all this information? And I will tell you that, you know, information, if it's available, will be used. And as it's used, it will raise very, very important governance issues.

So one of the reasons that we wanted to bring this privacy discussion here -- and we actually hope to carry it to Bali -- is because we think these issues are coming to a head quickest in Asia, and in many respects, because Asia is a little bit late to the show, they actually have more flexibility in terms of their discussions within government and with their companies to begin to adjust to a very, very different sort of emerging reality.

So I hope that, you know, one of the things that we can report out of this Internet Governance Forum is on privacy is that there may be a need to kind of rethink where we are. Not that we haven't achieved a lot and not that I think, quite frankly, that Korea has really kind of shown us the way in terms of really thinking through a lot of these issues. And Japan is going through a very, very serious process right now as well. But okay, where are we going to end up? And I think as Nir said, it seems like we're moving off in all kinds of different directions, and that's very worrisome.

So as usual, I've spoken too long. I think we've got room for just a few questions if you have it, but Carolyn will be available, Nir, Taro, and Hyun-joon as well as, to talk afterwards. I mean, I think privacy is one of the key issues where uniquely the Internet Governance Forum can claim to speak from a much broader group than governments, academics, or for companies.

So thank you. Any immediate questions or concerns that you'd like to kind of put on the record? Because there is a record of this.

Okay, then. Well, thank you very much. There's a chance at the reception to grab any one of these people, and I appreciate your attention and patience as we went through this. Thank you.

(Applause)

\*\*\*\*\*\*\*\*

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

\*\*\*\*\*\*\*\*