Singapore IGF – June 17, 2011: Session 1b

Cybersecurity, Privacy and Data Protection

Site: Suntec Singapore International Convention and Exhibition Centre, Room 303

Number of speakers: 6

Date: 17 June 2011

Start: 11.00a.m

End: 12.30a.m

Zaid Hamzah – Chair

Emcee: Welcome back, ladies and gentlemen. Now, we will start afresh for our second discussion for today, which is a very critical issue indeed in the daily lives of society and that is cybersecurity, privacy and data protection issues. I would like to invite the Chair, Mr. Zaid Hamzah to address the issue. He himself is a Strategic Lawyer Consultant.

Sir, would you please address the issue.

Zaid Hamzah: Thank you very much. We've got about one hour and a half to go through this session. I'll skip all those niceties about them being distinguished etc. etc. They have to prove their worth to you – we'll skip all the niceties.

Here's how I plan to conduct the session and give me your feedback on what you would prefer to see. I prefer closer consultation with the audience. I think the most important task that we have for this session is to frame the right issue.

I think I will try to avoid the situation where the speakers or the audience start listing issues out. They are important but we need to identify and frame the right issue. I've invited my speakers and I've given them a framework of discussion.

Now, the range of issues is on page 12. We're not likely to go through all the seven issues that I've identified but what I've asked the speakers to do is to focus on a few areas that can make a critical difference. We've got a broad topic to cover so I prefer a laser-sharp approach in identifying key issues.

Here, maybe I can share with you that I'm sort of biased towards the McKinsey approach where they look at things in the following way and I am hoping that my speakers will also address it along the following lines.

Number One: What are the drivers and the dynamics in the area of cybersecurity, privacy and data protection that directly have an impact on Internet governance. So, it's drivers, levers and enablers. Therefore it's important that we don't focus on any one particular issue but look at a range of issues that can make a difference.

You may hear from Kuek from Yahoo! Or you may hear from the Internet Society; you may hear from academics. But what is important is the outcome that we can derive from this session is that we can identify very clearly the principles.

If I can bring you back to the definition of Internet governance, the working definition: we are supposed to evolve shared principles, norms, rules, decision-making procedures and programs. So, no listing of issues – we'll look at the operating sphere that we are in. We will address issues such as balance, control, light-touch versus heavy-touch regulatory approaches and more importantly, if any of the speakers or yourself as the audience wishes to prescribe a certain course of action – provide the evidence for a compelling approach in relation to that.

With this sort of framework in discussion, I think the conclusion that I hope we can reach for today's session is that: Internet governance is really a soft science but if you think about it very deeply, it need not be soft skills area. It can be a strong management science and my hope is that by looking at the domain that we are going to deal with today – cybersecurity, privacy and data protection, we can actually develop a clear road map that can be forwarded for consideration in Nairobi.

Speakers will have 10 minutes each – I'll give them a polite reminder before they end. If they still continue like what happened yesterday – I couldn't believe it, 45 minutes – I'll just take the microphone away from the speaker if they don't listen.

With that, Kuek I invite you to do the first presentation.

Kuek Yu-Chang: To avoid an awkward situation where I'll have the mike taken away from me, I'll just do it without the mike but I hope everyone hears me. My name is Kuek, as mentioned yesterday, I sit on the Board of the Asia Internet Coalition and I know that there are many partnership opportunities out there. We have a lot of interested people and different groups who want to talk about Internet governance. I'm on the Board of that group and I welcome conversations on that but my day job is with Yahoo! and what I do at Yahoo! is to work on public policy issues. So, these are issues that as a company, we think about it a lot and we invest a lot of time thinking about it.

When you look at cybersecurity and data protection as I pointed out – these are all three very big issues – and I think we have a great panel today and we are all going to bring in something slightly different. What I would like to do is to bring an industry perspective to the discussion and genuinely talk about the mechanisms and the kind of relationships that are necessary to come up with regulations, perhaps or a framework that is feasible and practical for all users that will be affected by these very pertinent issues.

I'm going to start off by talking about 3 broad groups that are affected when you talk about cybersecurity, privacy and data protection.

The first thing: the first layer that we will naturally look at is government. Governments – we look to them to come up with right legislation, not too heavy, not too light and to come up with the right approach towards governing the Internet sphere. The natural question that comes next would be: Are governments necessarily in the best position to come up with different policies and legislations?

Yes, we do think so but what we feel is absolutely necessary though is that when governments or lawmakers come up with new laws, they make sure that there is a wide-range of consultations to get different views and practical issues out of the way when introducing new legislation.

I came from a policy-making and legislation drafting background myself and I was dealing more with the copyrights sphere and one thing we were grappling with was to make sure, or trying to make sure, that the legislation that results from all these consultations is technology neutral and yet at the same time, effective enough to bring about the right outcomes within the environment.

I think what has emerged from that discussion is that we have found that co-regulation model is probably one the best models that are out there. Governments, depending on their range of ability, might not always be able to capture the full technology behind something like the Internet sphere. Also, what I think is very important is that you don't come up with legislation that is so prescriptive that it hampers innovation that companies like ourselves think hard about. This is what I have to say about the government's procedure within this rule-making environment.

The other very important group to talk about when it comes to these issues would be users. I think I talk to many governments and I explain to them that if you go onto the Yahoo! Website – and I see Google and Cisco and other companies here as well – the Privacy Policy is up there; the Terms of Services is up there as well and users are fully informed of what they are

getting themselves into. One of the reactions that I always get is that, “Oh, come on, none of these users actually goes through your Terms of Services or your Privacy Policy before they use your service.” And then you pause and you go like, “Well, they should.”

If you think about a lot about these situations, the Internet is relatively new but issues such as security and privacy are not new at all. In an offline environment, if you procure a service or if you are going to buy something, generally I would think it’s a good idea to look through the contract or look through the company’s policy before getting involved in an activity. And I think users need to know that the same applies to them as well. I’m going to run through a few product features that we have on our website that works hard to empower users so that they give themselves the opportunity to be engaged in the Internet in the safest way possible. I think there must be awareness that it is their responsibility and the onus is on them as well to protect themselves.

I’m looking through the White House Cyberspace Preview and I think it makes a great point in saying that the government needs to do more in terms of public education so that users know how to protect themselves and know of the risks that they are involved in when they engage in the Internet. The second very big part of any rule-making process or coming up with any framework is getting the users involved and having them understand the kind of risks they are taking and there are on the Internet, very much similar like what it is in an offline environment.

Now, the third part that I want to talk about is the business perspective. For businesses, I think there are necessarily good actors and bad actors and there are people who invest a lot of time in thinking through issues; and there are some companies that don’t. For Yahoo! for example, we have something called a Chief Trust Officer. So you have heard of a Chief Information Officer, you have heard a Chief Operating Officer – we have something called a Chief Trust Officer and all her department looks at are things like privacy and data protection issues. She looks at child safety issues and so you have a higher resource looking at that specifically. Why do we do that? Simply because – as you know – people are going to come back and use your services only if they trust your product!

I’m a new parent myself so a lot of my analogies are about children and baby products. Think of an Internet company like a manufacturer of car seats. You will buy a car seat and use a car seat only if you are convinced that it is actually something safe. You will repeat buying their products or their toys only if you feel safe enough like: it doesn’t have a high lead content, the buckles actually work, the seams are not going to tear off the moment something unfortunate happens. It’s the same thing with the Internet as well. Companies; there are actors out there like us, who invest a lot of time having entire security teams look at security, who have entire teams looking at the user-facing end of the technology to make sure that users are empowered to make the right decisions.

And here is where my slides are. I tried not to put in too much, just to show you some screenshots of what is available for users when they use our products.

(Slide show)

The first thing I want to talk about is our security sign-in. This is a sign-in that I created for myself – this is one of the photo seals and when I see this, I know that I put the picture up there so I know that this is not a phishing site that put up a fake sign-in seal to get my ID. There’s also a pop-up sign that says, “Is this your sign-in seal?” to make sure that I am on a legitimate Yahoo! site and not some other pretend site. It says that you can change your sign-in setting and when you click that, what actually appears is that you are brought through steps to make sure that you design it in a way that only you would recognize it and that if someone was trying to fake a sign-in seal; then they won’t be able to do it. You can even put a picture of your kid, of your cat and frame questions so that only you know that you are putting your password in the right place.

Another allegation that I sometimes hear is that, “Sometimes when I go to your Privacy Policy, I know its on your front page, I know its on every single product that you have, and I know that its always on the same place and I can click it and understand your whole thing. But who’s going to read the entire document?”

Well, if you go to our Privacy page, it isn't one long legal document. It is like this and it is meant to be interactive. It isn't a scroll-through. It's customized to be user friendly. It goes into the features of our different products.

Something we also have – all these are from the Singapore site, I went to the Singapore site to get the screen grabs – for example, it also asks you that if you are going to upload information and make a comment; or if I'm going to put a photo of myself, it reminds you that:

"Please note that if you are going to write on the Yahoo! Singapore elections site and give comments on how you think the elections are headed or this party and that party, this is your photo that is going to be put up and this is your user ID that will appear for everyone to see." It will also remind you whether you are sure that this is what you want to put up. It is another layer to remind people of what they are getting themselves into. This is also a Privacy page where you make it very easy for people to opt-out and I see the cue.

This is a slide on self-regulation. This is just to show you that businesses themselves, work very hard to bring about the best outcomes, which is why I think a co-regulation model where industry has a constant conversation with the governments before introducing new legislation, is a feasible model and I will stop here.

Zaid Hamzah: Great. I'm going to be very strict about the timing. Now, just some key takeaways – technology utility, co-regulation, avoidance of innovation impairment and the Chief Trust Officer, which is key.

As Raj gets ready with his set-up, I really want to keep it short so that there will be a lot more time for interaction. Are you ready, Raj?

Rajnesh Singh: Good morning and since we have a very strict dictator in the form of our Moderator, I have to be grateful because I was actually contemplating not saying anything and just saying, "Whatever Kuek said" and end it there. But no, I need to talk about online privacy.

We have three topics, as it were, that we want to discuss today: cybersecurity, data protection and online privacy. To a large extent, all of those are interrelated and so what I'm going to do is concentrate a little bit on what online privacy is and how we are approaching it at the Internet Society.

(Slide show)

Most of you perhaps, would have see this: a little graphic which is one of my favorites and one I use quite often when I'm talking about cybersecurity and privacy and so. And what it says at the bottom is that, "On the Internet, no body knows that you are a dog." This was published in The New Yorker in 1993, some 18 years ago.

The understanding of course is we say that the Internet is a source of change, it's a revolution, it's dynamic but that cartoon from 18 years ago is still highly relevant today – In fact, actually even more so than it ever was.

On the taxi on my way here this morning, I had an interesting conversation with the taxi driver. He asked me what I'm doing and I said I was here for an Internet conference. He asked me then, "This Internet thing; its interesting how its changing the world." I said, "Yes, indeed it is."

Then he said, "One of the problems that I have with it is that now we only let our fingers do the talking." I said, "Well that is interesting because we use our hands as well."

The whole concept of social interaction is changing and what struck me is that we are now talking about that today so it was interesting whatever we are going to be talking about. I should actually add that we had a very interesting conversation and he didn't actually want to charge me for the taxi fare, which is quite nice of him, but I insisted on paying.

Compared to the traditional sense, what is it about online interaction that makes it different? It's a whole lot of stuff.

Number One, right at the top of this is no inhibition. People are less shy online because they don't have the face-to-face contact so the way they interact makes it much easier for them to share about what they want to talk about.

Of course, the lack of face-to-face feedback is a big issue particularly if we are talking about a cross-cultural conversation. We can't see facial expressions, we cannot really pick-up tonal expressions, and there is no body language so we cannot really guess what he or she is doing and so on. So we use of a lot of those little icons to portray our emotions.

Unfortunately, there is a lost in translation factor with that because when we are talking across cultures, different things mean different things to different people so we need to be very aware of that.

Unfortunately, there is also a very false sense of security and that basically leads to the disclosure of personal information and Kuek, of course, covered some of that in his presentation and how Yahoo! is trying to change that.

Then there is also the concept that all are equal on the Internet because there is no high-low, or big shot; poor or rich – it really doesn't matter because you just are a presence on the Internet.

So, what is online privacy? Here's something that we are suggesting is perhaps a definition of what online privacy is: sharing data in an explicit context with an expectation of scope. So when we say sharing, we say that the sharing is happening within a context rather than the prevention of sharing, which is when you want to secure something so there's a secrecy part to it. When I talk about context, it actually defines the situation in which we are actually sharing the data. When we talk about scope, it's about how exactly will that shared data be used.

Let me give you an example. Let's say you do online banking: you share certain information of yourself with your bank and in return your bank provides you with the information and the trust relationship between the two is the idea that it is being used with a specific context with a specific scope. So that is what we think the definition of online privacy is; perhaps, what we should be talking about. We have been putting together a couple of events in the last couple of months and I think we've been having good response to this so again we would appreciate your feedback on what you think of that.

Now, when it comes to security and all that, and how we get into this Internet governance business – there is no magic solution. No one is going to press a button and make everything go away or the security problems are going to go away. When it comes to security, and Internet security for that matter, it is about you; and me those around us; how we interact between us and of course, with society at large.

One thing to keep in mind is that privacy is not a universal concept. Privacy means different things to different cultures to different people. How we create privacy in Asia is very different to how the Europeans will see it and how the Americans will see it, and so on.

We also believe that it is not going to be solved by one tool. It really is going to be a combination of tools and some of those tools are: laws by the governments, best practice guidelines by the community, industry and so on; technology itself – things like what Kuek mentioned in his presentation; business practices – how do we do things; and of course, education – which perhaps is one of the most important component in this.

Because as more and more people come online, we need to educate them that you are entering a new world as it were but the fact is, it is also a big bad world and you need to be certain about what you are doing, what steps are you taking and what the consequences of their actions are. People get a bit haphazard, perhaps, when they get on the Internet for the first time.

Now, Kuek mentioned that governments and industries should follow the co-regulation model. I would like to suggest that you missed one part of that and that the users also need to be involved. It needs to be a multi-stakeholder process, so that means governments definitely; industries, most definitely; users; civil society; community groups – we all need to come together because this affects all of us. We are the Internet because we are the people who use the Internet.

Of course, what we also need to do is to try and balance this whole concept of security and privacy with other goals such as the free flow of information across borders. We said that they are not borders that there are no geographical borders on the Internet so we need to ensure that this remains so – otherwise the whole value of the Internet will change very drastically.

A holistic approach is required. We need to have an emphasis on consistent and inter-operable privacy frameworks and of course there comes legal, technical, business, social and so on.

We also need to keep in mind that usability is just as important as transparency and controls – we don't want to build a strong brick gate around the computer just so that we can control the user. Because then, it's not really usable anymore. We need to make it easier and easy as well so then, that poses a challenge for industries to see that users actually understand what they have been given actually makes sense and that they are actually able to use it rather than lessen the impact.

Therefore, Internet privacy cannot be considered in isolation. A better understanding of the intersection between privacy, security and reliability is needed because it's always a balancing act. We can make things very, very secure but it might have an impact on how it actually works and operates and how people are able to use it.

So, my strict Moderator has not told me to shut up.

Zaid Hamzah: You have four more minutes. I was going to take questions later unless it's so compelling – is it so compelling? Okay, I am persuaded by you.

Sheila Awat: My name is Sheila and I'm from Element 14. The question I have is about privacy on the Internet. For Asia, for Asia-Pacific in general, privacy laws are not very developed. I think the Internet is forcing most governments and regulators to govern privacy and data collection, usage and dissemination. Are we using this opportunity to encourage some consistent approach to privacy, data collection and usage?

Zaid Hamzah: I got to stop you because the question is not compelling so I overrule you – for one simple reason: I want to maintain the flow. It's a very important question and we will come back to it immediately after the last speaker. Thanks very much.

Kenying Tseng: Maybe my presentation can answer some of your questions.

Hi, my name is Kenying and I'm from Taiwan. I'm from Lee and Li, Attorneys-at-Law. For people from Singapore, you might think I'm from the other Lee and Li law firm but I'm from Taipei; we are the largest law firm in Taiwan so that's the difference between Singapore and Taiwan. I've been practicing e-commerce and privacy law in Taiwan for quite some time so today, I think my main contribution is to share on my experiences and observation in relation to the private practice, the interactive relationship between business and the users; individuals as well as how law and the statues have played an important role in protecting personal data and privacy.

Being a lawyer, some of the most frequently asked or frequently sought legal advice would be: How can businesses, be legal and liability-free, collect and use the personal data of their customers and potential customers? This is because business wants to provide services to its customers and they want to grow their business as well so they constantly need to collect personal data.

So, if you ask this question to me as a Taiwanese lawyer, I would advice you based on the Taiwanese Statues.

We have a Data Protection Act in Taiwan. The first draft of the Act was enacted in 1995 so it has quite a lot of history. Before, it used to only apply to certain areas and certain industries. But now, it was amended in 2010 – in the future, this Act will apply to all industries including the government sectors and also individuals.

So, this Act will first of all, create an important focus for the society to discuss the issue of data protection and also, some of the elements that have written into this statue can be a very important example for all of us to understand how the law can help to protect privacy and personal data. Based on this law, there are statues and concepts that I do not want to introduce yet, but there is a very important concept: that is, if you want to use or collect personal data, legally, then you basically need the consent from the individual – the consent from the data subject.

You may ask: What kind of consent would you need to obtain? There are many different forms. One way is that you can enter a contractual relationship with the data subject; you can enter into an agreement with the data subject and the agreement can be in oral or written form – they are all acceptable. Another way is you obtain a separate consent. When you are required to obtain a separate consent that means you intend to do something, which was not within your original intention of collecting the data. So, these are the basic principles under our law – you need the consent from the person.

Also, there will be subsets in the consent. The individual needs to consent to the scope of the collections as well as the scope of the usage. This forms the substance of the consent and the substance of the consent defines the future usage as well as actually defines the individual's privacy rights in the future.

You may ask: Will there by any restriction to the consent? Can the person just give out their consent freely without them doing anything else?

Our new Act introduced a new concept and it's for some sensitive data such as medical treatment, or DNA data, or the person's sexual life, health check or criminal records – for these sensitive data, even with the consent, with the written consent of the data subject, one cannot collect this data. So, there are some restrictions written into the law to limit the scope of the consent.

This restriction to the consent as well as the substance of the consent from the scope of the privacy – from this, we can learn one very important thing: that is, actually the protection of the privacy lies in the hands of the individual. If you give all your consent out, then you will get less protection on your privacy.

Also, in our new amendment of the Data Protection Act, there is another new concept that is: data obtained from a generally available source. This concept is quite new and is also quite difficult to understand from a lawyer's point of view. From our legislative intent, we found out that this consent was created in response to activities in cyberspace.

Across the Asia region, in Taiwan or in China, people personally would be searching for certain individuals. For example, recently we had a case in Taiwan where a girl in our MRT system did something very impolite to a senior citizen and they had a big fight in the MRT system. So, somebody else videotaped this case and broadcast it through the Internet and people started searching to find out who this girl was. Within a short period of time, this girl was identified and was under very great pressure. Eventually, she apologized to society saying that what she had done was wrong.

This is why our legislators thought that way about data from a generally available source: because people can just do a search on Google and Yahoo! and ascertain a certain person's identity. But if an individual allows his or her data to be thrown into these generally available sources, then this data would not be protected. Then this data would not be considered for privacy.

This is very important because when anyone wants to upload your data, you need to consider; at least think twice, whether you want this data to be known by the public and whether you want this data to become unprotected under law. This is very important for each individual to understand. But again, I think no ordinary people or consumers would ask this. How would we know when we upload any data onto the Net, for example, when we use our Facebook to interact with our friends, sometimes even close friends do not know how far your data will be extended or broadcasted on the Web because Facebook adopts a very complicated system for their Privacy settings? So, people would ask businesses on the Internet to provide an easier solution on privacy safety: Can't they just clearly tell the users what to do in order to protect their privacy?

Recently, another app developer approached me. They want to develop a social network application for iPhone or other mobile systems and we were asked to draft their User Terms and Privacy Statement. I was thinking along the lines of what Yahoo! has done but what can a business do to help the consumers understand what kind of data will be collected and what kind of data will become public in order to help individuals to protect their privacy?

Another driving force will be technology because modern technology has significantly lowered the costs of surveillance. I think for most of you, because we are frequent Internet users; you must understand that it's very difficult to hide your location if you are using the Internet. It's getting easier for the authorities or the governments to trace the identity or the location of certain Internet users. Because of this technology development, this can change the concept of what is public and what is private. If the data can easily be captured on the Net, would those data still be considered private? Technology can be another driving force for this.

But I think law can be another driving force to prevent technology from being abused. For example, in the legal system, there are some people who are creating a legal system to prevent such an abuse. For example, as I just said for our Data Protection Act, although the individual may place their personal data on generally available sources, the data might not be protected.

On the other hand, if you are using technology to monitor or catch or download data that is not generally available, that is you are using more advanced development technology, then maybe you are doing something that is not allowed by our Data Protection Act. The development of technology needs to respect what the law has set. Also, there are some other statues to protect public speeches. For example, we have the law to protect against the unauthorized services. We also have criminal sanctions on people who record on public spaces without the consent of the people joining in the dialogue. Those will become the legal restrictions and when technology develops, it must respect these legal restrictions so that our privacy and personal data can be well protected.

There are some actions that we can take – first of all, the actions of the government. I think the government plays a very important role in the protection of privacy. In short, continue to educate the public and the Internet users and encourage discussion and dialogue in society to form a common view and value of privacy protection. Here, I would like to use our Data Protection Act as an example. Our Act was amended last year and it will apply to the whole society. This actually shocked most of the individuals because in the future when you are using your cell phone you need to consider whether you comply with our Data Protection Act because you have all the cell numbers of your friends and your relatives. The amendment of this act actually highlighted these issues to the whole of society so right now, people in Taiwan are talking about how we should protect our personal data and in what way we can use or collect personal data.

This Act, although it has created some uncertainty, but the most value is that the whole society is now very alerted to the issue of data protection. Technology development can help – solutions that allow for anonymity should be explored. Incidentally, in Taiwan, we are discussing Cloud computing and one example is that we are using Cloud computing technology to store the medical records of hospitals and in case of emergency, different people can help the patient if they can get the data form the medical store. But then, people are worried that hackers get into Cloud and all the data is revealed. So discussion has been

developed on how these data can be uploaded into the medical Cloud without any identifying information so that even if the records were leaked, in an unauthorized manner, the people would still be protected. So that is one way that technology can help protect our privacy.

Another is that businesses has been collecting and recording a lot of personal data in their database. This creates a great security burden on each business so I think businesses now should consider whether they could carry less personal data in their systems in order to prevent any security issue.

That will be all for me. Thank you.

Zaid Hamzah: Bakar, we invite you now to do your pitch.

Professor Abu Bakar Munir: Good morning everybody. I was requested to participate in this panel discussion last evening so I put up some slides for this presentation and I thought I must touch on a few issues by showing you this.

(Slide show)

I think everyone in the room knows that Sony has been attacked not once, not twice but three times in April. And 100 million customers are affected and legal action has taken place in some parts of the world and action has begun; regulators around the world are also questioning Sony about their security measures.

This is another incident recently and it involves Citibank and again, regulators are asking or at least questioning Citibank about what they have done for their security measures. This is what the World Economic Forum recently acknowledged: that cybersecurity is one of the risks that the world will have to face in the next 10 years. But to me, its not only the next 10 years but perhaps more than that; forever!

After the incident involving Sony, this is what the CEO says, “Cyber crime is not a brave new world; it’s a bad new world.” With that introduction, I would like to introduce the subject of privacy and data protection because all the speakers have mentioned privacy – privacy online, privacy and so on.

The very general concept of privacy is the right to be left alone. But when we talk about data protection, basically we are talking about information of privacy. That said, information of privacy to some extent, can be attributed to personal data protection.

Why are they here on this slide? These are some of the companies who have problem with regulators over data protection issues. Of course, the list is not exhaustive. More and more companies are supposed to be here.

What are the international instruments? There are international instruments already in place, as early as 1980. OECD has come up with the guidelines of data protection among member countries or member economies – but of course, some of these are non-legally binding documents – including the APEC Privacy Framework and of course, the European Union Directive is binding for all European countries.

What other approaches do countries around the world adopt? One is Comprehensive Legislation; Legislation plus Self-Regulatory; Self-Regulatory and doing nothing. There are many countries, especially in our part of the world, which have done nothing so far to protect personal data.

What other countries have adopted Comprehensive Legislation? All the EU countries, Japan, Korea; I have Thailand here because they have come up with a draft; I have the Philippines here because the Philippines Congress is working towards it and Indonesia and China is there because they have come up with several drafts on data protection.

USA adopted Self-Regulatory approach plus Legislation: state laws and safe harbor. Safe harbor was developed because of a EU directive in 1995. Singapore adopted a Self-

Regulatory approach but perhaps it doesn't work and Singapore is now working on the data protection law and that is one of the reasons why I'm here.

These other countries, especially in our part of the world who have done nothing so far – Brunei, Vietnam, Laos, Cambodia and many more – are understandably, perhaps data protection security is not their priority. But Brunei and Vietnam are member economies of APEC and APEC requires member economies to do something to protect personal data.

Data protection around the world: blue – comprehensive data protection laws enacted; red – pending efforts to enact law and white – no law.

Some developments in Asia: Macau – enacted in 2006; China – has come up with several drafts and the latest draft was in 2007; India – amended their act and some new provisions on data protection is there; Indonesia – came up with a draft bill in 2009; Thailand – has developed a draft bill in 2010; Taiwan – as you have heard just now, amended the old law and passed on more concrete and safe data protection law in April 2010; Malaysia – has passed a personal data protection law in June 2010 and I was a party to that Act; Korea – came up with a more comprehensive law in March 2011; the Philippines congress is now debating the bill that was submitted; Australia and Hong Kong are in the process of reviewing their Privacy Act and their Privacy Ordinates respectively; and as I said Singapore is currently developing a new Bill now; and in April, interestingly, the EU Working Party has decided that the New Zealand Privacy Act is adequate as far as the adequacy requirements of the EU Directive is concerned.

I'm coming to the end of my presentation. These are some of the key features of data protection laws around the world. Basically there will be data protection principles, rights of data subjects. For consumers, there will be exemptions and normally there are two types of exemptions – one is total and one is partial. If you collect data for primary reasons, for primary purposes then you are exempted. If you collect for recreational purposes, you are exempted. Data in relation to security or economic affairs of the company or country are normally partially exempted. Of course, enforcement mechanisms will have to be in place and then you have sanctions.

In Australia, except for one situation where it involves credit-reporting amnesties, the rest of the sanctions are civil, same thing in New Zealand. In Malaysia, all are criminal – the Personal Data Protection Act of Malaysia has created new criminal offenses. In Hong Kong, it is civil plus criminal offenses or sanctions.

Now, we have come to data breach notifications. Recently when Sony was hacked, one the issues raised was: it took Sony two weeks to notify customers. Was that too late or was that okay? Sony was arguing that two weeks is okay. The regulators are saying that perhaps it is not okay. Citibank took one month to notify their customers. So, again the same question to be asked is that is that okay? And the second question is that, who should be notified – Customers or regulators?

When I look at the Philippines draft Bill, the notification is the customers as well as the regulators. In Taiwan, when I look at the Bill or the Act of Taiwan, interestingly the notification is only to the customers. Not to the regulators. This is an interesting issue to be debated. With that, I thank you for your time.

Zaid Hamzah: Thanks very much, Bakar. Now, may I suggest – I want to make sure that there is a nice wrap-up to the issues. So, could the audience now start thinking of the issues that you want to ask? I'm going to do it this way because it's going to be a bit random – think about your questions ahead so that immediately after your presentation, we can proceed.

Lim Yee Fen: Hi, thanks. I must apologize to Bakar because I was the one responsible for inciting several people yesterday to get him to speak today because I thought that with him here, it's just such a wasted opportunity if he doesn't speak. For those of you who heard me yesterday, I will not be speaking at my bullet train speed, as you will be pleased to know.

Basically, in addition to my law background, I actually more so, was a qualified computer scientist and I worked as a computer scientist in my previous life. Until recently, I was also privileged enough to teach as a full professor at a law school here in Singapore, but now I'm actually with NTU.

I specifically asked Mr. Chairman if I could be last because I wanted to try to wrap-up and give some thoughts on Internet governance especially in relation to data protection. I think the first thing we all would agree on for anything in Life, is that prevention is always better than cure. Whether its medical problems or whether its security problems and in terms of cyber crime, there are many ways to combat cyber crime and obviously, one of the ways is through good security – because if you don't have good security, then you are asking for trouble. It's like, how many of your leave your cars unlocked? Unless maybe, if you leave in New Zealand. We used to be able to do that in Australia maybe 20 years ago but we can't anymore.

Basically, security is one way and another way, which unfortunately lawmakers and citizens alike do not really connect with cyber crime, is data protection or more loosely, privacy. And I was very pleased to see that Bakar had set up the difference between privacy and data protection because they do mean different things.

Being a lawyer, I am pedantic and I tell that to my students. So, what then is data protection? When I asked my students this earlier in the year, and these are law students, the brightest of the brightest in Singapore, these undergraduate law students, all they said to me was data protection is just to keep your data secure. I said, "Wrong" and they were shocked that data protection extends as far back as the collection process, the recording, the organization and the re-organization, the adaptation, the alteration, the retrieval, the consultation, the use, the disclosure, the dissemination etc. etc.

Basically, what I want to do is to give my take on five main points in terms of what are the best approaches to governance in terms of protecting privacy and protecting data on the Internet. As I said, I have five and I will probably start with the first and if the bell rings then I will just skip to the last because I've listed them so that the first is the most important and that the last is the second-most important.

The first is really a top-down and bottom-up approach – because I think people need to learn to not just simply hand out their personal information about themselves. The two main categories of people that I have in mind here are probably the first of all, the young, because they are probably the most prevalent users of social media such as Facebook – but that's not to say that they are the only ones who are happily giving away their personal information and their personal data because the second group are the general citizens.

Like I said yesterday, I am Australian and I've been here for four years and I'm actually quite surprised at how easily Singaporeans just handover their personal information. Its been reported in the Straits Times here in Singapore that a lot of surveys done here simply say that Singaporeans simply don't care about their privacy and I think that is what I mean by a bottoms-up approach because people need to be more aware that they are giving away very, very valuable information about themselves which can be used to harm them.

There are businesses – I'm not going to mention any names because we are on a web telecast because I do not want to be sued upon landing in any country – but there are businesses who have in the last decade or so, have built their businesses and develop business models based entirely on encouraging people to give away their personal data.

They have gone about this in a tactical and strategic manner so that they portray it as normal. They are trying to change the social norms. They are trying to say to you there is no such thing as privacy because this is a digital world – that is just a whole lot of garbage because at the end of the day, data protection is not about secrecy. It's about control.

Yet, there are these companies, and I have to say they are mainly technology companies who utilize the Internet and they have built billion dollar industries around people's personal data

and trying to tell people that this is a very normal thing to do; and its a good thing to do and so on and so forth.

For this bottom-up approach to take greater effect we actually do need a top-down approach because we need governments to set-up some minimum requirements in the laws so that you can actually change the mindsets of the citizens, change the mindsets of the businesses and the organizations. This doesn't mean that overnight; we are going to have a wonderful, big Data Protection Act. It can be baby steps in legislation. For example, in Australia, we started out in the 1980s with a Privacy Act that only applied to the private sector but then with the EU Data Protection Directive, we then moved to the public sector. But then, there are problems with that because there are a lot of exceptions – Australia is still not compliant with the EU Data Protection Directive.

Basically, what I'm saying is that there has got to be top-down; there has got to be bottoms-up – and even if its top-down, I know that some governments, especially in the region, are concerned about compliance costs for them as the government as well as for the businesses, especially the Schools of Businesses. But all I'm saying is that they only need to be baby steps.

The second point I want to mention and I think its already been highlighted by some of my co-speakers is that there must be public and private sector involvement; and there must be the involvements in these two sectors both in the application of the law as well as in the regulation. So it's got to be in the way that it applies and in the regulation. Personally, I don't think self-regulation works that well for privacy. We can just look at some of the problems that the US has faced in the last 20 years and you will see why. I think co-regulation is actually a very, very good model to explore especially in the region where we do want to encourage economies and so on and so forth.

My third point in terms of governance approach is with sanctions. I think they should be a combination of civil and criminal sanctions because it gives greater variety and choice to the people because if they just have a regulator or agency overseeing privacy, it really ties the hands of individuals who have been aggrieved by data protection.

The fourth point is application. Like if we have a data protection – whom should it be applied to? Basically my personal view is it should be applied to both commercial and non-commercial because in Australia – I am Australian so I come from the Australian perspective – we have had all sorts of problems with some of the exemptions. In Australia, for example, we have exemptions like political parties – they are exempted from data protection. So you see a lot of abuses that goes on in terms of personal data in that area.

My fifth point is you really, really must have a breach notification law. Basically, if there is a breach, you must require the organization or the body to report it. This is quite essential but unfortunately, this is not at all prevalent in Asia. It's not in prevalent in Australia and its not prevalent at all in Asia.

So, they are my five takeaways in terms of my approaches to Internet governance. I just want to wrap-up. Just stepping back because we are in Asia, and this is an Internet governance forum for Asia Pacific region – just some general observation: stepping back, if we look at Asia as a whole, quite a number of countries do not have any data protection laws at all. Some do have some laws, but they are sectoral and they are so sectoral that they may only apply to the banking industry so it's practically useless. Some have comprehensive laws and I was sniggering away when Bakar said, "Oh well, Australia is under the comprehensive law." Well, yes and no. On the one hand it is comprehensive because there was an effort to comply with the EU but there are actually a lot of glaring holes in the regulation if you look at it. So on the one hand, it is comprehensive but really, not that comprehensive at all.

The last thing that I want to note in terms of Asia, or Asia Pacific I should say, is that I don't think any of countries in Asia Pacific have cross-border transfer regulations. I think that is important and this was first brought up in the EU Protection Directive in Articles 25 and 26. But I really, really, think its quite essential because in a lot of countries, they do outsource their call centers.

For example, in Australia, we have had a lot of problems with banks outsourcing their call centers to India and other places. And once you outsource, that means your banking data including your bank account balance, the transactions you have had, your personal address - its going offshore and if there is no regulation about it going offshore then you have a problem. Its like saying that we might have regulations within Australia, but once it moves out, who knows what the people in India or the hackers in India or the employees in their call centre in India is going to do with your data. I think that its really, really important to have cross-border trans-regulations but as far as I'm aware, I don't think any Asia Pacific country – and that includes Australia and New Zealand – has any cross-border transfer regulations.

Thank you very much.

Zaid Hamzah: Here is what I plan to do for the audience participation. For those who want to stay longer, beyond 12.30pm, I will encourage you to do so, so that we don't have to close this off just because. I'm not going to adopt that.

I will give the opportunity to those who want to ask a quick question and leave for lunch on time. Can I first have a show of hands: who wants to ask an issue other than that lady who will be the first to repeat her question? Who would like to raise issues? Can I just have a show of hands so that I know how many questions are going to be asked? Four – it's like an auction here. Anymore hands before I close? A usual courtesy reminder – please provide your name, your organization and then the issues, as short as possible.

Sheila Awat: I didn't record the question but my name is Sheila Awat. I come from Element 14 and I'm the original Council. The question essentially is that the Internet expansion and governance gives Asia Pacific an opportunity to focus on privacy and data protection, which we have not focused on in the past because of the speed and size of data.

My question is: In all these studies of privacy, data collection log, has Asia Pacific governance for these or APEC or similar forums focused on trying to get some similarities across the different jurisdiction on privacy and data protection laws because its very varied and very incomplete. Thank you.

Zaid Hamzah: I won't ask all the panelists to respond. I'll just ask two but if anyone finds it so pressing to give me your inputs, please do so. I just want to manage this better. I think Bakar and Yee Fen will be the best two to answer.

Professor Abu Bakar Munir: In one of my slides I have showed some international instruments and APEC Privacy Framework is one of them. So APEC has come up with some parameters, some perhaps basic principles that member economies have and should adopt when they develop their domestic legislation. So, the answer is yes for Asia Pacific. At least for APEC member economies, there is a framework that has already been setup in the APEC Privacy Framework.

But of course, the APEC Privacy Framework doesn't make it mandatory to have legislation. It talks about legislation, administrative and other measures to protect personal data. So yes, there are some parameters set up by the APEC Privacy Framework. Of course, countries are free to look at the OECD guidelines or even the EU Directive, if you wish. But the EU Directive is very stringent in its requirements.

So the answer to your question would be, yes.

Zaid Hamzah: Let's proceed with the question from the back first then proceed with Sala.

Shoba: Hi, my name is Shoba and I'm from the National University of Singapore. I wanted to ask – we talk a lot about empowering users and educating users, especially. But Eli Pariser's in his recent book The Filter Bubble has talked about the concept of lock-in. That what happens is we want to use a particular product, let's say Facebook for example, and you've invested so much in it; your whole network is on it and everything so even when they have these huge privacy infringements, its too hard to just move out of Facebook and use something else.

What I want to ask is the point of view of businesses like Yahoo! for example, that try to be ethical: how much can you really empower users? How much can you really educate them because even if you know that you have all these options, you can't get out of it sometimes because you are forced to use it.

Zaid Hamzah: Great question – that's definitely for you.

Kuek Yu-Chang: Thank you for your question. I will avoid commenting on other companies but I think you do see some trends. Some businesses have been around for longer, Yahoo! has been around for 16 years there are other companies, which are younger and might have a different approach or are more aggressive on certain policies.

I think what is great then is that if you make sure that information is made available to users, and I think we talked about that a lot today – that users are educated on the risks that are involved and what they are getting into when they put their information out there and know that the onus is on them to make an active choice to use products that they are comfortable with. This is the number one key.

The second thing I think is – and we did talk about co-regulation – is that when you push these kind of reflective mechanism and put the onus on the companies to think through their policies, and what we commonly understand as good or bad policies, I think it becomes easier for users to identify which companies think hard about these issues and hopefully, users are entering with their eyes wide open.

I do get your point that when a certain company reaches a certain level of dominance, that people might find it hard to get out of it. I would try not to over-state the situation because this is a very rapidly moving industry. I mean, 4 or 5 years ago, has anyone Tweeted or anything? There are things, which were big, just a few years back – like IRC, ICQ – so I would not over-state the fact that people have choices and that people do move away. I do get the point that – and I'm sorry but I haven't read the book yet – but I agree with the point that is being made but I don't think we should overstate that. I hope that answers your question.

Zaid Hamzah: Thanks very much. Let's take Sala's question followed by the lady at the other end behind and then, Harry.

Sala: Hello, I am aware that this forum is Asia Pacific regional IGF and issues that come from here will go to Nairobi so I think that its critical that I raise this on behalf of what's happening back home. I happen to chair the Fiji Cyber Security Working Group so we work closely with the Ministry of Defense and surprisingly, among the stakeholder group comprising of Telcos, ISPs and banks, financial intelligence units, transnational crime unit and also OCU and other regional organizations.

We hosted a first multi-stakeholder workshop recently, we had remote streaming and had experts from Germany also tuning in and very good feedback was brought in from different industries. Essentially what we tried to do was create a buy-in.

Now, linking it back to discussions from the panel, one of the interesting things that I picked up that is critical is – I will first refer to Mr. Singh from ISOC. His presentation was that it is critical that we engage in a multi-stakeholder approach and consider the users.

I'm just speaking from personal experience, but not too long ago, a friend of mine who was with me at home, her Yahoo! account actually got hijacked. Because I work with cyber crime and I am in cyber security, the first thing I did was emailed investigators in the cyber crime unit to lodge a complaint. The second thing I did was I went to the Yahoo! site – by the way, I am not attacking Yahoo! as this is just to discuss issues – and I lodged a complaint but the thing is we got no response.

The nature of the email – she's a friend of mine who is also a lawyer; she works for a bank – which had been sent out to all her accounts, and this was when she was with me when her Yahoo! account got hijacked and I received this on my phone was: I'm stuck in London and can you please send me some money.

The first thing I did was I Googled that city – I looked for the nearest police station and I sent an email to complain and because London is faraway it took them about 24-hours to send a response – and they replied saying they were sorry but they don't deal with this sort of complains and all kinds of issues.

What I am trying to say is that this personal experience exemplified and personified to me the issues. It is transnational; it is something that has to be examined holistically and microscopically. By the way Professor, in June I was browsing through BlogSpot and I enjoyed both Professors' presentation.

Getting back to the point, because I know that you will take it to Nairobi right?

What I think needs to happen is that social utility or multi-national organizations like Yahoo! or Facebook – wherever they are, it is critical that whoever regulates them, if they have a license that this should be – if they are not internationally held responsible – local laws apply to them, primarily.

My reasoning is, if say Yahoo! is in Asia or wherever they are registered, it is in my view that the duty of the regulator who is issuing the license to make sure that the necessary provisions that protects consumers. It is critical also at some level to discuss how internationally; those issues can also be addressed because it's no good if it's not addressed domestically.

Zaid Hamzah: I hear you very clearly. I've actually taken note of it – it's very, very important. In fact, if I can seek your help later on when I do the summary, can you just join me? I definitely want to bring your views across.

Next question from the back.

KK Lim: Hi, my name is KK Lim from NYP – I'm not an academic; no. Previously when I was a Chief Privacy Officer for a US company, as I travelled around Asia, one of the reasons that regulators, including Australia, one of the important points that regulators will bring up for not implementing the Data Privacy Act and whatever was the cost of breach notification.

This question is open to the panel. Now, breach notification is not cheap and therefore the regulators are resisting it because they don't know how to handle this component.

The second question is addressing this issue is about cross-border issue. The cross-border issue is largely solved according solved according to some regulators and it's essentially solved by some technical controls. For example, if you use Citrix, then when you login, all the parts are encrypted. So it's the issue of technical control and that is usually the answer the regulator will post to people like us that go around persuading to adopt data privacy Data Protection Act. We solved that by technical control.

But breach notification, how do we handle that cheaply? The question is cheaply.

Zaid Hamzah: I will pass to Raj first. I think Raj can take the middle line followed by the business followed by academic – a very quick intervention by each of you.

Rajnesh Singh: The cost of breach notification? If you find the answer, let me know.

In terms of technical control, one of the things that the Internet Society is currently working on is what we call the Trust and Identity initiative. The whole concept we have behind that is: How do we actually build trust and authentication into the network design itself?

It's a bit too technical to get into right now but I think it's an interesting body of work that we are working on right now, so if you are interested in that I can pass you some information, which you may look at. Basically, it's all about building trust and authentication into the network architecture as opposed to work on it after you have started using it.

Lim Yee Fen: I'm going to abstain from the breach notification because I am assuming that you are going to say something about it. I just want to say something about the cross-border – I think you may have misunderstood what I meant. It's not so much that it may be leaked

during transit but rather when it gets to India. So for example, the bank account holders' information about Australians – What do the Indian people do with it? If the Indian people or employees or hackers start breaching it, there is absolutely no recourse for Australians with bank account information that has been compromised. That's what I meant by transfer; its not so much the technical side because the issue is more at the level of how you protect data once it gets into foreign hands where you have no jurisdiction over them; where the courts can't get to them and where there are no laws.

Zaid Hamzah: I will get Kuek to answer two questions, including the one by Sala because you must have the right of reply, albeit quick ones.

Kuek Yu-Chang: I will try to make this quick. I think data breach is very important and companies like us definitely want to do the right thing. For example in South Korea, the law has been passed and now we are trying to figure out the details of the decree that will prescribe the law. We are in conversation, right now, with Korean legislators on what data breach legislature should look like – what's the trigger, what's the format, how do you notify people.

One thing that Yahoo! believes in is that the most natural way, for example, to do the notification is through the format that the user has used the product. So, email for example. Having something sensible like that, instead of making sure that someone calls you or making sure that you get something is writing, for example, is a practical way that is sensible and perhaps can address some of the cost issues that we are talking about. I don't want to say too much and pre-judge the ongoing discussions but I think there is a way out and conversations on that are happening.

In Sala's anecdote – well thank you for the feedback. This is something that is useful for us to hear and this is something that I will take it back to Customer Care. Having email accounts being hijacked is a problem that has affected all companies. I think Bakar had referenced a few slides – thank you for not putting the purple Y-band logo on your slide and I hope that Sala's intervention doesn't change your slides. Your slides are great the way they are.

I think there are so many learning points from just this conversation. You are an example of a savvy user who knows how to deal with the situation and we just need to make this education available to all users so that they know what the appropriate way to respond to this is.

Even though in this case, it is specifically an online problem, people are very familiar with such scenarios in an offline environment so even though having this come through your email pertains to the Internet environment, people have been dealing with this in an offline environment and people need to be savvy about how to approach these things.

Zaid Hamzah: Thanks very much. You can take it offline. Before I ask Bakar and Raj to give their points, Harry, I want to hear from you. Those of you, who want to leave for lunch, go ahead because I just want to keep the interaction going.

Harry: I just want to focus the discussion on recent development. I am tempted to follow Yee Fen and say I'm not going to mention the name of the organization but I think I have to. Facebook came up with this new technology called facial recognition.

I am sure the panelists are familiar so I want to ask a specific question regarding that because if you take it in the context of a business organization that is global that has got many millions of account holders and you then take the stacked folder regardless of how they are sold – whether they are allowed users or not – and allow them to adjust pictures setup by strangers and have their names which they have no control over this tagging.

In context or RGIF, which is what this whole forum is about – its about regional governance: How would you advice the members of ASEAN – in Asia Pacific as you have mentioned before, a lot of us don't have any privacy or protection – how would you advice people within these countries if they are going to start thinking about creating something or developing their laws, which way forward is the best? I don't think any body of law, whether it's a combination of self-regulation and legislation is able to control something like what Facebook has done. I

just wanted your feedback – if there are others here regarding their point of view regarding Facebook face recognition software, I would like to hear it.

Zaid Hamzah: Thank you very much. Since I still have most of you, what I'm going to do now so that everybody can hear the question and the answer – I've got three pending responses – why don't I hear from the lady at the back. Let's give her one last opportunity before we wrap-up.

Vindoo Shama: I'm Vindoo Shama and I work with the International Centre of Missing and Exploited Children. Our issue is that of illegal content. And the question we put up here because we do work with Yahoo! in the US and in Australia is: How do we deal with illegal content, and in our case, specifically with child pornography issues. Where does this fit in with this industry debate? We are all talking about data protection and privacy laws but there is a huge amount of this illegal content in cyberspace and who is addressing it, and how?

Zaid Hamzah: Great, we will take that as the last question. Let's start with Bakar first; Raj as an intervention and then I may ask Kenying if she wants to, to reply to the question relating to the specific legal issues.

Professor Abu Bakar Munir: I will try to give my comments on KK and Harry's questions on breach notification. I must admit that not only breach notification issuance will cost money to the company but also to comply with the whole Act on data protection can incur cost for companies and organizations in the country.

But I would like to look at it from a bigger picture, a bigger perspective. How about the fact that the country does not have any laws whatsoever to protect personal data? Is it good for business or is it good for the country?

I would like to think that having data protections laws can make a country more competitive and there are compelling reasons for businesses to comply – to have data protection laws and to comply with the data protection laws.

Back to breach notification, I don't believe in law trying to solve all the problems. To me, it must be a comprehensive one involving the technical, educational as well as legal. So, the law is not the silver bullet in this case.

About Harry's question on the latest initiative or latest product of Facebook – what I can tell is that recently, this issue was raised in the EU and EU regulators are asking questions to Facebook and in fact, opinions of the EU Working Party is that it might be in breach of the EU directives.

Zaid Hamzah: Thanks Bakar.

Rajnesh Singh: I'm going to refer to one of my colleagues on the panel here. You mentioned India a few times so I think you might be happy to see that the Indian government enacted some new legislation, specifically on privacy and data protection among a whole lot of other things. It was done in a very quiet, somewhat stealth manner. Basically what it means now is that if an outsourcing company for example – if we go by the letter of the law – if its processing data for whoever, there has to be explicit written consent from the user that they can process that data. Now, that has created a huge problem, which is just emerging as people are realizing what the law actually means because essentially, the whole outsourcing industry will collapse if that law is applied and regulated by the government. So what they have done is gone from essentially no legislation and no regulation to the direct extreme of it.

There are user rights issues coming up, there are privacy issues from users coming up as well – basically it means that intermediaries are being affected. There is a 36-hour notice to meet and this means that within 36-hours, the problem has to be fixed. There are data breach implications, which involve the shutting down of websites, preventing someone's access to it – so we have gone right to the extreme end and that is quite worrying as well.

I think trying to find a balance – that is going to be the heart of it.

Zaid Hamzah: Kenying, do you wish to answer the issues raised by Harry? If so, then I will ask Yee Fen to deal with the last issue related to content. Would you?

Kenying Tseng: In response to illegal content on the web – in Taiwan, we have tried a few different approaches.

A few years the government tried to launch a content rating system in Taiwan for each webpage where businesses needed to put the rating on their page to show whether it is acceptable for children to view or not.

But this is has not been successfully launched because it is very difficult to provide a unified rating system especially of content over the web. Many websites are nationalized so the Taiwan government is still finding a way to properly rate or mark the content.

Another way, which is what they have done, is to place the burden on the ISP or ICP like Yahoo! so we have been helping the Taiwan Yahoo! to communicate with the government for this kind of liability issues. They try to place this burden on ICP, to hold them liable if somebody else places illegal content on their websites. But here, I think the burden will be too much for an ICP because people are placing these content on their own and its difficult for them to monitor this as well.

Right now, the principle is if they are notified and then they will have to take it down. For example, for copyright infringement, if the ICPs have been notified and they still do not take it down then the ICPs will be held liable. This general mechanism has been implemented further; for the Internet Group, they still think that the government has not done enough because of the restrictions of technology and the huge amount of data on the web. Maybe, we can borrow the solution, which we have discussed for privacy – we need a co-regulation system and a top-down and bottom-up approach to achieve the purpose.

Zaid Hamzah: Thanks.

Lim Yee Fen: I was just going to say that what this system really needs is data security and what you mentioned is a broader species of cyber crime, which some jurisdiction just lump under content regulation. Australia is one of them. I have to say that apart from child pornography, it is going to be really hard to find another area, which is universally prohibited in every single country in the world because there are lots of disagreements about what is objectionable content, but I think child pornography is one of them.

As for the responses, I actually think there is a lot going on in terms of the law enforcement agencies like Interpol and in terms of Australia, I know certainly a lot of the federal agencies, a lot of the federal police have been working with a lot of other federal police organizations around the world and they have cracked some child abuse rings and child pornography rings. That's that.

I also just want to make a couple of comments here. I mean, Raj is absolutely correct to say that India has recently introduced laws about data protection. I think India is probably what I would call an example of a big baby step. Whilst it has got laws, it might not be entirely comprehensive because for example, it only applies to the commercial entities and I think it could be, in some respects be regarded as sectoral. But that is an example of a jurisdiction, which has taken a big baby step, and I think that that's all we should be striving for, at the very least for the time being.

If every single country can take these steps, however big or small, then it's a step towards better data protection and better cyber security.

Lastly, I just want to address Harry's question. I didn't want to mention any names but I will say that since you mentioned Facebook, with my class of law students, we spent a whole week on Facebook studying its policies, its actions and past actions.

There are really two things that I would say to a regulator. The first is: Facebook consent because as a matter of clause, Facebook rarely ever gets consent from its users. Secondly,

it's the Default settings because more often than not, if you go into your Facebook, the Default settings have always been against the protection of the users' data.

I think there was another comment I wanted to make earlier on where there was a lady who asked about whether it is realistic because a lot of these services on the Internet – if you don't want to use it, then you are basically locked out. I think in a way that is true. But we must not enlarge the problem. For example for Facebook, I just told my students, "Don't use it". Unless they get their Privacy Policy and Privacy Settings correct, then don't use it. I personally do not have an account on it. And if you do want to, then you breach their Terms of Service and don't put your real name, you don't put your real date of birth and you let them sue you for breach of Terms of Service if they really want to do that.

At the end of the day, it also comes back to user help. As we all know, Gmail has used automatic scanning of emails for a long time. So what that says to you is that you simply don't put private things on Gmail email. Thanks.

Zaid Hamzah: There is a request from Kuek first, but is it a pressing question? I will let him answer first.

Kuek Yu-Chang: I just wanted to latch onto the issue of child pornography because this is something that I know my company thinks about very strongly and I personally am very passionate about that so I just wanted to comment on that.

Yahoo! as a company treats takedown notifications for child pornography very, very seriously but it's an interesting space because you have to balance two things. One thing is legitimate request for takedown and yet at the same time, being a believer of the open Internet, and making sure you do provide facilitative approach to legitimate content. I think the regulations – having takedown notices – that's one thing but another thing as well is that companies should proactively go out and educate their users and make sure that things are kosher in that kind of environment. In all Yahoo! front pages, together with our Privacy Policy is our Safety Policy where you go in and it teaches you about how to teach your children what are the right things to do; how do you protect yourself against cyber bullying; how do you protect your personal information – that's something we do.

Also, three weeks ago, I was at Ho Chi Minh city and I concluded an MOU with Unicef and what we are doing is going out to the schools to help in the trainers program so that children at school are in a position to know that they are going onto the Internet and that they are a new to Net user and I am going to do this or that so I should be aware of this or that.

I think another approach is getting the structures and legal frameworks in place and another thing is that we need that kind of education to users again, that there are certain things that you just should not be doing and I'm a strong advocate of that.

Zaid Hamzah: Thanks very much. One last question and we will call it a day.

Sala: I came to this forum to talk to people to see whether their respective countries, whether they categorized it. I know Australia categorized their cyber security; I know Council of Europe has categorized; the US has categorized; New Zealand hasn't and Fiji is in the process and interesting to say, that demarcations for example, in Australia, they have theft of telecommunications services categorized under cyber security.

Just another point I would like to make is – in general, in terms of whatever I've learnt about juris-prudence on the matter is that a crime is only a crime if there is a specific code that says, if you do this, then this will happen or you are not supposed to do this. In other words, I would say that the child online protection and pornography and all sorts of illegal content falls into the greater realm of cyber security so she's actually spot on in raising that question.

The real issue is: Have countries in Asia Pacific categorized it, which I am sure there are different answers to that as we all come from different contexts. If they have categorized it, how has this been translated into laws in terms of criminal laws and criminal codes – whatever it is in Arab and Egypt?

Interesting to see that the Egyptian model – I know about the revolution in Egypt but what most people didn't know is that the Telco's had no mechanism for categorizations and that sort of thing. So, when is cyber security a threat?

Back to point I'm trying to make, what are the different categorizations? I will be very interested to know what is happening in Singapore.

Zaid Hamzah: Thanks very much. I really value all your inputs – with that, let's show a round of applause to the panel.