Internet Governance Forum
Hyderabad, India
Open Dialogue
December 4, 2008

Note: The following is the output of the real-time captioning taken during Third Meeting of the IGF,
in Hyderabad, India. Although it is largely accurate, in some cases it may be incomplete or inaccurate
due to inaudible passages or transcription errors. It is posted as an aid to understanding the proceedings
at the session, but should not be treated as an authoritative record.

>>MARKUS KUMMER: Good afternoon, ladies and gentlemen. We're here for our second open dialogue session. It is rather a big room, and there are many people right at the back. We would suggest that they move forward a bit to create a more cozy ambience.
Before we start, I have an announcement. We had some participant who had one of the more than thousand backpacks that are around, and he lost his own. And it includes his passport. Otherwise, it's no -- it says it's the usual stuff everybody else has in. So please check whether you have his passport. His name is Mawaki Chango. And he also has a network power in there. But I think the passport is the most important thing. And should you find it, please hand it back to the lost and found desk.
Also another announcement. We have checked with the registrations, and we have now 1273 registered participants. That includes 133 media.
[Applause]

>>MARKUS KUMMER: Which is, all in all, I think, a very good show-up, considering the circumstances.
Are we ready to start? Okay. Then I hand over the microphone to Jonathan, who is our moderator for this afternoon's session.

>>JONATHAN CHARLES: Good afternoon. Welcome to the session. Thank you very much, indeed, Markus (No audio).
Of the IDN, which is cybersecurity. And all the issues that raises to do with the balance between security and privacy and threat to the Internet from many areas (No audio).
You have probably been in the sessions this morning. If you haven't, don't worry. We're going to get the rapporteurs on the two sessions to come and give us the full input of those sessions so we know how -- this is really your chance to get your input. What we're going to do is, if you want to make a comment, you'll stick up your hand and we'll bring a microphone around to you so you don't have to queue up at the microphone. I'll pick you out in the audience and have someone bring a microphone to you and make your point.
I'm very keen that we stay on topic, that we move through this logically, and that (inaudible) that you make comments that are appropriate to that particular point (inaudible).
We will move forward to conclusion and come back (inaudible) and try and (inaudible). These debates are much better if they're focused on the issues that are being discussed at that time.

And if you react (No audio).
Cybercrime, though we know what that is, we know there are millions of viruses out there. We know the threat to the net. We know that real pessimists say that if these issues are unchecked, that the Net itself will fail five years down the line or ten years down the line or maybe five months down the line. So great threat.
What we want to come up with today, I suppose, is to try to work out some of these tradeoffs between security, on the one hand, protecting ourselves, and the need to keep the Net dynamic and open, where (No audio) -- the balance lies on that particular part.
And also what role can we play here in the IGF on trying to take the debate forward and trying to come up with solutions to what has seemed quite an implacable problem.
I'm going to start by introducing one of our co-chairman here. We are joined by Gulshan Rai. He is director of the Indian computer emergency response team. He's going to say a few words. Then we're going to hear from the rapporteurs from the two sessions today. Then we start throwing it open to the debate, to you.

>>GULSHAN RAI: Thank you. We have the open session -- we had the plenary session in the morning where we talked about the cybersecurity and cybercrimes over there. We had chairman, and the second session was also very important for the security. This was chaired by Mr. Shyamai Ghosh and reported by Mr. David Gross.
It very clearly emerged that the Internet and the mobile telephony are the two important discoveries of the 20th century there. It has made a great impact on individual life. And, in fact, these two technologies are inseparable from our day-to-day life.
But then what happened that has it brought a real potential, have we realized the full potential of these two technologies for our societal application or society?
Today, we have more than three billion mobile connections in the world and more than one billion Internet users in the world.
The -- as I said, we still have to realize the potential. The reason is the lack of trust of the user in the usage, particularly the e-commerce and other financial applications there.
The user is worried about the cyber threats, like virus forms or trojans or identity theft. The organizations are worried about the stealing of data.
The infrastructure, critical infrastructure, is worried about his data (inaudible) or the malfunctioning of the infrastructure.
In the session which I was a member in the morning, the -- it was emerged that there are five pillars of cybersecurity. Alone, the legal infrastructure or technology is not the answer. We have to looked at integrated manner, if we have to keep the trust of the user in the applications, because we expect this one billion number will definitely increase to number of billions in the time to come, maybe in five to seven years.
The five pillars which were identified were the legal measures, technical and procedural matters, the organization structure, the capacity-building, and the international cooperation. This in fact has to be looked at an integrated manner if we have to provide a safe and secure cyberspace to our citizens and to users, they have to put trust in that.
This session is an open session where we invite each and every one to put forward his views, put forward his comments. And the session is open to all.
I give it -- with these comments, I give it to Jonathan to conduct this.

>>:Jonathan Charles: Thank you very much, indeed.
Before we go on, let me introduce my co-moderators who are over there on the left.

Closer to me is Natasha Primo, who is national ICT policy (inaudible) in the association for -- sitting (No audio) is recall at the Brazilian embassy in Washington, D.C.. He is vice chairman -- I'll try to speak up -- vice chairman of the GAC and a representative of the Brazilian government. Their job is they're going to intervene regularly. They're going to keep an eye on some of the questions. They're also going to pick up on some of the salient points, as they said, and move us on from time to time. It's not just questions, of course, that you can pose by sitting in your chair. You'll all have been given pieces of paper. They're going to be collected by the ushers. If you want to write down a question, then feel free to do that. Write down your name. Write down the question. Hand it to one of the ushers, and they'll bring it to us at the front. And we'll also probably be taking some questions from our remote access audience, from people who are watching us at various hubs around the globe.
Let's start, then, by just recapping on what were the main points of the two sessions today, which we had earlier today, on cybersecurity.
First of all, let me call on Bertrand de la Chapelle to actually tell us the main points from one of the sessions this morning.

>>BERTRAND DE LA CHAPELLE: Thank you. Just rapidly, a few points as we've agreed to have five bullet points basically.
The first one is the notion of prevention, not only remediation, prevention, proactive measures to make attacks and exploits harder and have a more resilient architecture.
The second point is the notion of a feedback loop between prevention, analysis of incidents, and remediation, the three feeding in one another to increase the awareness and increase the knowledge about how to respond to attacks.
The third thing that has been used a lot is the notion that there are a large number of actors that are involved in the prevention, the remediation, and all those issues. They are from all categories of stakeholders. And the building of trust networks among those actors is essential, and it requires time, and it really requires to base them on the relationship and the trust among them.
The fourth point is the notion of avoiding to address issues in silos of actors and avoid having the governments on one side, the private sector on the other side, and civil society or other actors on the third side, and the technical sector. But, rather, to organize discussions on an issue base, to get people by categories of incidents, categories of dangers, categories of problems, and bring all the actors together in a multistakeholder (No audio) -- is the notion of organizations, the brought frameworks and having broad frameworks doesn't necessarily mean a (No audio) -- but agreed (No audio) that was suggested. One theme was the question of the cost of security.
Another theme was raised by somebody who belonged to the software development sector about standardization of security issues (No audio).
The third point was the role of the IGF on this issue and why it is and how it can be appropriate space, what role it can play. And the last question was raised was -- is the role of the various organizations that are dealing with those issues in various regions, in various categories of actors and how they can interact with one another, just to feed into the debate.

>>:Thank you very much, indeed. Let me call on our other (inaudible). You were at the other session. Give us the rundown of the five main points from that session.

>>:Thank you, Bertrand. So, yes, we had a really nice and interesting debate during the second panel of the morning. And if I have to resume and find out with five points, the first one will be (No audio) -- in the debate on (No audio).

>>:I think we're losing you.

>>:Okay. It's better now?

>>:Yeah.

>>:Yes. I was saying, on our first point, the role of the Web 2.0 in the protection and preservation of privacy, security, and openness, and particularly what social networks are affecting or how privacy is related to these new technologies.
And a second point, the importance of freedom of expression and access to information and global information flows and how to keep preserved and enhance those rights in the Internet.
Then a third point on the importance of information literacy, on being able to use those technologies to understand the potential and the risks of those technologies.
And a fourth point, how do we deal with different cultural, legal frameworks across countries.
And the fifth point, if, in the debate on privacy, security, and openness, we have to confront several stakeholders. How can we find a common ground, and how each one of the stakeholders with his role can help draw a line and define the spheres for security, privacy, and openness. So those were the five main points. So I hope in this debate we can have further discussion on those. And interrelate with the session on cybersecurity.
Thank you.

>>JONATHAN CHARLES: All right. Andrea, thank you very much, indeed.
I'm going to start by -- maybe we should -- it would be useful to have examples. Maybe you've had to deal with it (No audio) -- for example, I had one only the other day in which I discovered something on my credit card for a very large (No audio) what had happened was that my card -- sold to an Internet site where criminals actually trade card details. And it's then being used to make a number of other transactions. That's just one example of -- another example of Internet crime where a Web site is being set up (inaudible) -- join this Web site using passwords, and they then swap details to use in a variety of places. That's just one example of cybercrime, one of the cybersecurity issues.
Anybody here have any other example. If you'd like to put up your hand. This gentleman down here. We'll get you a mike.

>>:We have multiple such examples. I run an ISP with, like, 40 million users. And every time I keep running across people who forward into spams and (inaudible), for example. One gentleman actually was very upset with me that our filters blocked his e-mail, that it was sending all his credit card details to Nigeria. And he was like, why did you stop me? I have a business deal that's going to earn me about $100 million, poor man.
Anyway, there's one stakeholder I think that did not get mentioned here, and it is a stakeholder that has been making the news for quite some time, at least one registrar believed to be owned by cybercrime operations and one large-scale Web host, that's domains and MC (saying name) were taken down because of articles in the Washington Post by Brian Krebs which basically had detailed exposés on the cybercrime links that were associated with these groups. And the media is one organization that helps those bridge between industry and civil society, it is a way to quickly disseminate

information.

>>:An educational element.

>>:Yeah. It's not just educational. Based on investigative reporting and based on his work --

>>:I use education in the widest possible sense.
Okay. The gentleman there. We'll just get you the microphone.

>>CHRIS DISSPAIN: Thank you. I think you -- hi, Chris Disspain. I think you asked for some examples of security.
How many people in this room have got a computer open?
And are connected to a network. And how many of you are connected to something called "free public Wi-Fi" because that's not the network. That's someone's computer. And there will be at least four or five of those in this room right now. And you could very easily have your computer connected directly to somebody else's computer, which means they can see what you're doing.

>>:Right. That's a good example.
Gentleman over there.

>>STEPHEN LAU: Stephen Lau from Hong Kong. Let me look at some statistics and quote some U.S. statistics. As far as identity theft or people as individuals' personal data got compromised. The latest are the survey from the FTC, Federal Trade Commission in the U.S., say that 3.8% of U.S. adults have been -- had their identity compromised or identity theft. 3.8% translates to 8 million people in the U.S.
So this is a really very prevalent, very wide kind of problem. And I think the business community, we have been reminded by various business organizations, including BASIS, ICC, that business organizations have not only to respect personal data of its customers and its employees, not from the point of just because it's a right of an individual. It's only just because compliance to law, because a lot of countries have laws to deal with infringement of personal data privacy. It has to be treated as a business imperative, as a business issue. It is a business differentiation issue. It is also a competitive advantage issue.
The reason why I'm saying that is, various surveys have looked at the issue of data bridges, which are becoming more and more prevalent in this world. And everyone of this data bridge, on average, would cost the organization, apart from branding issues, reputation issues, cost in terms of transaction, in terms of regulatory punitive measures, costs about -- I can't remember the exact figures, but it's absolutely in the millions. I think it's three to four million per episode.
And we said this morning, in Internet, trust is the issue. It's not price. It's not cost. It is respect, and it is trust. And so you have a trusting culture respecting your customers, respecting your employees' personal data, that it would help a lot. As I said, not only in terms of cost, prevention, but also in terms of reputation and branding, as well as a business imperative and business differentiation.
Thank you.

>>:Stephen, thank you very much, indeed. Stephen Lau.
Any more examples of people who have been either suffering cybercrime or have dealt with it in some way? Yes, it appears, that gentleman in the back with his hand up

there.

>>:Good evening. I am (saying name) from (saying name) Hyderabad. I'm (inaudible). When the government top director requested me, he has received an e-mail threat from an unknown person from Yahoo! stating that he is misusing his (inaudible), and the mail was addressed to the superiors of the authority.

>>JONATHAN CHARLES: Can I ask you, sorry, just to hold the microphone much closer to your mouth. Because we keep losing some of your words.

>>:Okay. The -- one of the top directors of the company has received an e-mail telling that he is misusing his authority, and the copies of the mail has been sent to his boss. In fact, he has lost a lot of mental disturbance because of that e-mail threat. He's unable to focus in his day-to-day operations. And he wants to track down, trace who has sent that e-mail which is disturbing his entire business, daily work schedule. So this is a total misuse. He is unable to trace down who has done this damage, which is unwarranted.

>>JONATHAN CHARLES: Right. Okay. That's an interesting line.
Let's go over to the left here. Two people, I think, want to speak. Gentleman, yes, in the suit, first of all, in the dark suit.

>>JONATHAN CHARLES: Right. Okay. That's an interesting one.
Let's go over to the left here. Two people who want to speak. Yes, gentleman in the suit. First of all, in the dark suit.
If you could just stand up and we will get you the microphone.
Very good. There's one coming over to you right now, at high speed.

>> (saying name), federal prosecutor in Brazil. And Mr. (saying name) from (saying name), an NGO in Brazil.
We usually have two different approaches regarding security on the Internet.
Infrastructure threats and human rights threats.
More than computers, the Internet connects people.
We all agree that human rights are universal and defined by international standard and treaties and must be respected and protected worldwide, including cyberspace.
National and regional legislation was sanctioned in order to protect human rights, which means to protect and fight against their violations.
It's not matter about one right versus another. It's a matter of how to protect these rights in a global view.
Moreover, as Mr. Gulshan Rai has observed in this morning's session, in five or six years, another billion people will access the Internet worldwide.
These new users come mainly from developing countries, like India or Brazil.
How to protect the security and the rights of these new users, especially children and adolescents considering that, one, crimes have been committed by nationals who take advantage of the borderless nature of the Internet to violate fundamental rights.
Second, despite the efforts of constraining the cooperation among law enforcement agencies, the current instruments of international cooperation are not efficient in order to cope with thousands of cases involving, for example, distribution of child pornography using international services provided by Internet providers based in the United States, like Google, Yahoo!, or Microsoft.
Third, unfortunately, the self-regulation model which has been successfully

implemented in Europe has not been working well in developing countries.
Fourth, despite all the risks that countries can use their power to violate human rights, including freedom of expression and human rights.
Under the international law, the states still keep the responsibility to promote and to defend human rights.
Therefore, concepts like sovereignty are not totally old fashioned in the Internet world.
For this reason, we, members of the Brazilian federal prosecution service and the NGO Brazil have been arguing that under certain circumstances it is totally legitimate to enforce local offices of transnational companies to comply with our own legislation and jurisdiction.
We believe that the situation in Brazil is paradigmatic because it creates a new form of creating social control and governance, balance between law enforcements, users of data requests, application of national legislation and jurisdiction, and big international ISPs, worldwide policies and strategies. Reflecting on the Google's Orkut case in Brazil can help us find the balance between preventing and reacting on cybercrimes and protect freedom of rights and democracy in developing countries.

>>JONATHAN CHARLES: I am going to be a really horrible moderator this afternoon because I don't want you to put your hands up unless it is directly related to the bit of the topic we are discussing right now.
Because we have a long way ahead of us and we are going to try to take things in a logical protection. If you have something to say on the topic, fantastic. If not, wait to the next one. I'm sure you will have something to say on the next one.
One last lady over there.

>> Just to follow on what the gentleman said about rights. I would just like to extend it to talking about the rights and freedoms of women and bringing the issue of cyberstalking. That's a cybercrime; right?

>>JONATHAN CHARLES: Do you have an example of cyberstalking?

>> Yes, there is the case of Amy Boyer, I believe was her name, a woman who was pretexted. Information about her was sourced from a man who then used that information to get access to her stalker, and it resulted in her death. A very well-known, well publicized case. So if we could just put that on the agenda as well.

>>JONATHAN CHARLES: Yep, definitely. And we are going to be talking about rights in the next hour or so.
Before we go on and look at what we need to promote cybersecurity and trust, let's look at one more thing, which is if you sit here and think what is your worst fear about what could happen to the Internet unless we tackle this issue of cybercrime, what comes into your mind, I wonder if anybody has any thoughts as to where they think this is going to end for the Internet unless we do something on cybersecurity.
Anybody like to put up their hands or where they think, the damage they think would be done to the Internet if this is not resolved?
Gentleman here.

>> People will simply be too afraid to use the Internet, though right now, cybercrime has always been it happens to somebody else, it happened to a bloke I knew somewhere.
Not many people, the vast majority of Internet users are not victims yet.

But this is likely to change, and it's likely to change for the worst if cybercrime continues to be uncontrolled, and as we see new people, new crooks deciding that cybercrime is a viable option for them.

>>JONATHAN CHARLES: Anybody else got any worst fears as to where they think the Internet is going, what is likely to happen to the Internet if this is not resolved? Gentleman over there in the white shirt on the left-hand side.

>> I would be concerned that, as new users come onto the Internet, the first thing that they will see is criminal activity, and they could very easily come away with the conclusion that that is what the Internet is for and that it's acceptable to continue to engage in criminal activity online.
I think that's quite a bit of what we have seen, unfortunately, with the folks in Nigeria or who claim to be from Nigeria.

>>JONATHAN CHARLES: Okay.
All right. Well, I think we know, then, what's at stake. We set out what's at stake. At a moment, we're going to start looking at where we might go with that.
Let me turn to my co-moderators. Everton, I think you want to say something.

>>EVERTON LUCERO: Thank you. Thank you, Jonathan. I think all the examples that were given were perfectly valid, and they show the complexity. Situation. And of course there are many more.
I would like to pick up on some points and perhaps based on your last comment on damage to the Internet, I just would like to emphasize also that it is important to concentrate on the damage to people. Because, of course, we all want the Internet to be safe, secure, reliable, but most of all we do not want the Internet to be an instrument for criminals. I think that's one basic notion that perhaps we could explore together.
Just picking up on the comment that was made by the federal prosecutor from Brazil, and if you allow me, I would like to mention -- take this opportunity to mention that it is an example of a national solution or an attempt to find a national solution, bringing together the social -- the civil society and the law enforcement agents, the lawmakers, because the way that it was possible to get to an agreement with Google, that runs Orkut, a very popular service in Brazil, on a term of conduct to fight child pornography was precisely through a special commission of inquiry at the Brazilian federal senate, which also brings us the idea of the important role of parliament in democratic societies in trying to frame this issue.
Of course, a national approach will not be a solution applicable globally, but it is a start and perhaps this will also be a case study for others to continue.
But I just would like to suggest, Jonathan, that I say here a suggestion that everyone who speaks identify themselves and where they come from and what they do before they speak, for the sake of the debate.
Thank you.

>>JONATHAN CHARLES: No anonymity here.
Natasha, do you want to say anything about anything that has grabbed you so far?

>>NATASHA PRIMO: Well, what I would like to suggest is that we also take some examples of how people have had their access to information blocked. Let's not just talk about cyber stalking, cybercrimes, but also what implications that has for different

groups and individuals in accessing their rights.

>>JONATHAN CHARLES: Yes. So we will do that.
Let me -- I think everyone here agrees -- Is there anyone here to doesn't agree --
Let's take a little straw poll. Everyone here agrees there is a problem, I take it.
Everyone here agrees that something should be done. Put up your hand if you believe something needs to be done about this problem.
Something should be done about this problem.
Okay.
Put up your hand if you think nothing needs to be done about this problem; that somehow, it will resolve itself.
Bertrand, you think there's a third question. What is it?

>>BERTRAND DE LA CHAPELLE: Third question, is everybody aware of what is being done?

>>JONATHAN CHARLES: Third question -- good question. Is everyone aware of what is being done?
Okay. And is everyone working together?
The answer is, it doesn't look as though there's much unity here. There's no unanimous approach, so let's start down our track of trying to work out where we need to go in order to improve cybersecurity.
And let's start with the question which I would like you to stick up your hand and try to answer, and I will come to that -- very quickly, that gentleman there.

>>ALUN MICHAEL: I am just a little bit worried about the set of questions. Of course we don't all know what's happening. The point of the morning panel I think was very good in giving a pretty comprehensive view of a lot of things that are being done. It was useful for that point of view.
Most people don't want to be aware of everything that's being done. What they want to know is that they are safe and that their concerns are being dealt with somewhere.
And that's why I made the point this morning that we need to build up from the national level the use of national level IGFs, which is one of the developments we promised last year we would do in the U.K., involving government, parliamentarians across party, industry and civil society. And secondly, looking at the bad side of the Internet, the criminal activity but also the low-level nuisance activity to say what are the things that people want -- dealt with and how do we manage to do that through a partnership approach, not a legislative approach which we know won't work.
So I think with respect -- in the cracks between your questions is where the real action has to be.

>>JONATHAN CHARLES: That's fair enough. And I will identify you. I think you are Alun Michael; right?

>>ALUN MICHAEL: Yes, Alun Michael. Member of parliament U.K.

>>JONATHAN CHARLES: Please make sure you identify yourself and where you are from.
There are lots of things that need to be done. We are not all aware of what's going on, and some of us aren't sure of how to proceed down this road. Let's start the debate proper. Let me start with a question, which is who do you think should be responsible

for improving cybersecurity? Does the responsibility lie with me, the user? Does it lie with companies? Does it lie with government?
Where does responsibility lie in this? And in what way does responsibility lie?
That's what I would like to hear from you all on.
First of all, there is a gentleman at the back standing up. We will get you a microphone, if you could identify yourself and say where you are from.

>> Good afternoon, gentlemen. My name is Freder. I work for an anti-virus company from Finland. I am from (saying name) corporation.
The question is who is responsible for ending cybercrime?
If I am allowed to talk, I would talk a bit about your previous question: Where is this going to end?
Well, Internet is a playground, as I say that. It's for good people and the bad people.
So however much we secure it, there are still people who can break it, because all this is written by human being.
So anything that is written secure, can also be broken.
It's obvious that all the viruses, all the malware, whatever is spread on the Internet is also a software.
So an anti-virus company is trying to break into that software and stop it from entering into your computers or the network.
So it's a similar human brain on the other end who is trying to break your antivirus software. So it is a software-to-software game.
So there is no end to it, and one thing that I would say is that there isn't going to be any serious harm that's going to be done to the Internet by these things, but it's going to be an ever lasting thing. An antivirus or a virus, good and bad, everything is going to exist, like the human beings, it's the Internet.
The same thing.

>>JONATHAN CHARLES: Where does responsibility lie, then, for improving security? Who does responsibility lie with, do you think?

>> The responsibility lies in no government, no organization, but the individual who uses the Internet.
See, there are two things here. One is enforcement. The other thing is education. And both these things put together could do a bit of improvement, but not 100 percent.
So education is important, enforcement is also important.
So what is to be enforced? There should be some body which works universally, should not have any country borders, no country law should be applicable for Internet because if I write a bit of content, a piece of content on the Internet on a particular Web site, or it could be offending for some countries, it could not be offending for some others.
So what should be the -- I know the deciding factor to say whether a particular piece of content or a particular act on the Internet is legal or illegal. So there should be a party, a governing party, which does not have any geographical boundaries. So the moment you're hooked up onto the Internet, you're no more a citizen of India, no more a citizen of U.S. The day I think someone starts working toward this, then I think we'll see a beginning of the end to the problem.

>>JONATHAN CHARLES: Thank you very much. Thank you. Maybe (inaudible). Lady here, I think you wanted to say something. Yes, we'll get you the microphone.
If you could identify yourself.

>>ANNE CARBLANC: Thank you. My name is Anne Carblanc, and I work with the OECD, but this is my personal opinion.
I think that, first of all, the leadership in fighting cybercrime should lie with governments. But governments are not the only actors. They need to work in partnership with the others.

>>JONATHAN CHARLES: Just let me question you, one question coming back on that. What is it you think governments can do, bearing in mind that they may not be acting on an intergovernmental level or are you suggesting they need to act on an intergovernmental level?

>>ANNE CARBLANC: Well, governments are the best place to identify and devise an action plan. And they need to facilitate coordination at national level, with the private sector. And responsibility lies with each actor as concerns cyber criminality.
This morning, people said that users need to also consider -- realize that they are part of the Internet and take minimal measures to protect their systems and networks. And governments also need to cooperate with other governments. So it's kind of vertical or intranational and horizontal across countries.

>>JONATHAN CHARLES: Okay. So we've got one person who's in favor of governmental, and one person who is not in favor of governmental intervention. Gentleman here.

>>SURESH RAMASUBRAMANIAN: Did somebody forget the word multistakeholder?

>>JONATHAN CHARLES: Right. Go ahead. We haven't mentioned it. So go on.

>>SURESH RAMASUBRAMANIAN: I know, I know.
I would hardly accuse the OECD of forgetting it, because you have the OECD tool kit dating back to 2005, which was one of the earliest models of multistakeholder cooperation and joint action against spam specifically. But most of the principles would apply for cybercrime and cybersecurity in general.
And the point is that there are several very fine, very workable models available that make a lot of sense on multiple levels.

>>JONATHAN CHARLES: Give us an example. Give us an example.

>>SURESH RAMASUBRAMANIAN: The OECD antispam tool kit, as I said. And the ITU has some very fine projects, such as a botnet medication tool kit and a readiness tool kit that a country can take to assess how ready it is in terms of combating cybersecurity.
And there are several other examples, such as a series of best practices put out by the messaging antiabuse working group, MARK, which is an industry group.
But best practices are not very useful as long as they are on paper or as long as the only people who are following best practices are actually the people who are already doing the right thing.
We have got a whole lot of people in developing countries and in developed countries that need to be reached out to and that need to be anything from educated to perhaps, in some cases, pressurized into following, by community sanction, shall we say, into following best practices.
And these multistakeholder models actually need to be taken out of paper and

translated into actual work.
I'm glad to see that this is happening. But it's happening very slowly. It needs to take place much faster. That's about it.

>>JONATHAN CHARLES: Okay. Thank you very much.
Please remember to say your name and who you represent when you speak.

>>SURESH RAMASUBRAMANIAN: Sorry. Suresh Ramasubramanian. And among other things, I am a consultant developing a botnet medication tool kit for the ITU. I also work for one of the largest ISPs in the world. And I run an NGO, antispam NGO, in the Asia-Pac that does capacity-building and policy and technical issues for local people. That makes me neither fish, flesh, nor fowl.

>>JONATHAN CHARLES: That makes you very multistakeholder. Thank you very much, indeed.

>>EMILY TAYLOR: Emily Taylor from Nominet, the dot UK Internet domain name registry. An observation is that many of the speakers seem to think that somebody else should hold the responsibility for sorting out security. And perhaps echoing the point made by Anne from the OECD, I think this is a shared responsibility in which each actor has a part to play.
I think there is a role for best practice sharing.
As the Internet is a new, emerging issue, people are doing what they can on the grounds to combat issues as they come up. And sometimes solutions will be formulated by industry. So, for example, our "Best-Practice Challenge," which we did this year, highlighted the example of Barclays Bank PinSentry, which has been very effective in combating phishing and has also been adopted in South Africa and in Turkey. This is an example of how developing best practices can actually helping. It doesn't solve everything, but if people can do their bit to take responsibility for what they can see and what they can affect, I think that this is a good model.

>>JONATHAN CHARLES: Yeah, perhaps I'm a Barclay's customer and it's an excellent security tool that's made a big difference. Lady over there in the blacktop, we'll get you a microphone. If you can say who you are.

>>LIESYL FRANZ: Good afternoon. My name is Liesyl Franz, and I'm with the Information Technology Association of America.
I'd like to build upon Emily's remarks and say perhaps the question isn't who is responsible, but what are the roles that the various players have in securing greater cybersecurity for the users, whether they be individuals or companies or governments, because all three we do have to recognize that those are the three various types of users.
So what are the roles of each of those constituencies in protecting their part of cyberspace, whether it's something that they provide to others or whether it's something they -- is determined by how they use the Internet, whether it's for citizens' services, whether it's for their own social and individual consumerism, or whether it's for their business operations.
So I think that -- really, what are the respective roles is really the question.
So government normally has a coordinating role or a law enforcement role or an intelligence-gathering role. And industry has a role in developing what the tools and solutions and services are for their clients or customers. And it is basically that

innovation and that provision is something that we definitely need to preserve in any of the efforts that we take or we wouldn't have the services that people are using. Productivity, efficiency, that's all part of the program that needs to be preserved as well.

One thing that we have talked a little bit about is the responsibilities of the users, whether it's an individual. And that social behavior is something that, unfortunately, some malicious actors do take advantage of. So providing educational opportunities for people to understand how to behave on the Internet, like the poor gentleman who thought that he was going to make a million from the Nigerian -- presumably a Nigerian Internet scam. That's very difficult, because it is such a widespread user base. But it is an important aspect as well.

So what are the various roles? And then, importantly, how do those players interact to be able to address the spectrum of Internet use, then the various aspects of cybersecurity from prevention, detection, when there's a problem, to, when something actually does happen, how you manage that incident, and then how you prosecute the malicious actor. So each player has a role to play. And in interaction, integration with the others.

>>JONATHAN CHARLES: Okay.

>>:Thank you.

>>STEPHEN LAU: Stephen Lau, Hong Kong. I just wanted to pick up a point, is, if we are talking about a law enforcement issue, and even though it is a multistakeholders, as mentioned early on, I, as a citizen, will look for leadership somewhere. And for law enforcement issue, if I cannot turn to my government and ask for help, then I think it will be very sad for any particular occasion or jurisdiction.

Now, the problems that are very complex is the border, multiple stakeholders and all that. But I like to feel that the government has a very important leadership role in terms of responding to the citizens' law enforcement issues.

>>JONATHAN CHARLES: Do you feel the governments recognize that now?

>>STEPHEN LAU: Oh, heck, yes.

>>JONATHAN CHARLES: With any capability, though, as opposed to feeling it with impotence?

>>STEPHEN LAU: Are we talking about -- first, are we talking about leadership, are we talking about sort of as a law-abiding issue, I think government has a role to play. Now, how do we actually enforce, how do we solve a crime, how do we accord, now, that's a separate, separate issue. And to follow on that, I hope later on we can discuss an issue.

This morning, we were talking about an incident reporting, incident investigation, it's very complex, transborder, cross border, and multiple roles and all that.

Now, I am here to learn. I like to listen to experts who have been involved in investigating law enforcement of cybercrime.

The strength of any endeavor is as strong or as weak as its weakest link.

From your experience, from those who are the experts, could someone tell me from their experience where is the weakest link? And if we know that, we can then address it.

>>JONATHAN CHARLES: Okay. If someone knows that, that would be very good and they can stand up.
I think there was a lady there in the green who would like to say something.

>> Thank you. My name is Manjima. I am an independent consultant. Right now I am here with the APC.
I actually like the word that this lady used which is how the governments respond rather than enforce.
As a user, I would like to know if I face a situation of cyber stalking or cyber harassment, where do I go? Who do I report to? What are the channels I have? Do I go to my local police station? Is there a special department? Are they online? Is there a number?
Moreover, what is the process? What is the procedure that will be followed?
My point is basically that other than regional sharing of best practices and online activity, off-line are governments prepared with a system, a mechanism, an infrastructure, do they have the expertise, the people to respond to these situations?

>>JONATHAN CHARLES: Okay.
That's an interesting one, isn't T it is the question of definition as to where criminality lies and where responsibility lies.
I will give you a quick example before we go on to many other people who want to comment.
I had an e-mail the other day from a social network that I belong to, Linked in, and it was a message sent to my personal e-mail from somebody who left a message for me on Linked in and this person wrote on Linked in, they put their name and they said, "We used to date in Spain before you got married." And they then went on to say, "However, I now understand you have married X and you have children X and Y."
I had never heard of this person before. I have certainly never dated anyone in Spain.
But they had somehow exploited the whole Internet resources to find out a lot about me.
They had found out the name of the person I had married. They found out the name of my children.
They had -- And then I put two and two together, and someone alerted me a few months ago to the fact someone was asking a question on Yahoo! questions, do you know the names of Jonathan Charles' children?
So people have done a lot of research.
Now, is that a crime? No. Or it might be.
Is it a cybersecurity breach? Certainly.
And there's a real gray area, isn't there, in all these issues.
And what to do about it and how to proceed on these issues.
Gentleman there, yes, with the microphone.
No translation).

>> My name is (saying name). I come from China Internet association. I am a Secretary-General of the association.
I would like to utter the Chinese voice. Concerning the issue of security, I fully agree with the idea that multiple stakeholders -- that is the government, civil organizations, companies and users -- should jointly share responsibility in resolving a problem. For example, the government in resolving cybersecurity issue, it should stipulate the rules. Well, for enterprises it should deal with the technical issues concerning the

infrastructure establishment. And concerning several organizations, their focus should be on coordination and communication. Of course, for users, they should have some ability to defend themselves.
And in China, concerning anti-spam issues, inspired by the forum starting from 2006, we initiated a multistakeholder initiative.
In the first place, our association did something concerning this Spam issue. For example, we asked the enterprises to strengthen their management of the issue and relevant rules and regulations were promulgated.
In March 2006, the government issued a law concerning this issue, which specified what is computer Spam, which in a way tells the society that this is something that violates the rights of citizens.
In this process we also organized enterprises and produced a black list, revelation of people who are involved in these kind of activities, and furthermore, in order to help the enterprises to deal with the issue, we have established a technical and other ways to identify these problems.
This is to ensure a smooth operation of e-mail service.
Also, we did a lot of -- issued a lot of cards to tell people how to identify the Spams and how to deal with them.
On the part of the enterprises, they have improved the training concerning operators up to about 1,000 people.
And starting from 2006 to 2008, in the course of two years, China's Spam constitutes about 20% of the world's total, and by the year 2007 it accounts for about 5% of the total volume. We can see it is a rather dramatic reduction.
This is a result done by SOFY (phonetic), a famous company in the U.K.
I want to share that a multistakeholder, joint action is very important. Of course there are other issues to resolve concerning cybersecurity, like concerning a lot of technical issues, like Bet Net which affects people's confidence in cyber.
This is a focal point of where we should work. And this is will show that in the future the forum might establish a kind of mechanism to coordinate our efforts in this area in the future, to establish rules concerning the black list, concerning the share of the responsibility, and concerning our joint action in this area.
I believe this is the next direction we should go so as to give substantive progress in our work in this field.

>>JONATHAN CHARLES: Thank you very much, indeed. We will discuss what the IGF might do a little later on.
Before we take even more of your comments from the floor, I think Everton wants to have another word.

>>EVERTON LUCERO: Thank you, Jonathan.
The more we hear, the more it gets clearer to us that no solution fits all; that this is a huge, complex issue. And that it has to be taken on broadly environment, with all the stakeholders, and also with shared responsibilities.
But perhaps we could, to guide the debate, think of two -- of a first division of possible issues to be taken, and on short term and long term.
On the short term, we have seen the challenges to law enforcement at national jurisdictions because today, as we all know, it is only governments that are able to enforce the laws in their own jurisdiction, as we don't have a global one.
And so that's one, a first set of issues that we need to address. How to overcome these challenges to law enforcement.
But we also need to think on the long run. And we have said from the beginning, we

have heard from the beginning suggestions regarding education, related to education. And I think we could explore also a little bit, in the long run, shouldn't we work better on how to evolve, how to have quality education? And now I remember Mr. Abdul Khan from UNESCO this morning, he also mentioned that education was one of the pillars of the knowledge society.
By the way, I know that most of the panelists of the morning session are present, and perhaps eventually you could ask them to contribute and further develop their ideas in light of the comments that were made.
Thank you.

>>JONATHAN CHARLES: Natasha, is there anything that strikes you from the past few minutes?

>>NATASHA PRIMO: I would just add that maybe one of the ways to take the debate a little bit further, and picking up on some of the ideas around the responsibilities of industry, for example, is to explore how, currently, the different industry players are pursuing a secure Internet agenda while also holding in balance other rights, rights to privacy, free flow of information.

>>JONATHAN CHARLES: Yeah.
Let's bear in mind as we go on to further comments, let's bear in mind the last comments of Natasha, because we are all very keen, aren't we, to protect our rights and our privacy on the Internet.
And one thing we ought to be considering, and I ask you to consider this, is where does the balance lie between our personal privacy, our personal rights, and the need for cybersecurity?
Because in some ways, there is a tension between improving cybersecurity and continuing to protect our own personal privacy.
It would all be a lot easier, wouldn't it, if we all had to register to go on the Internet and say who we were. That would make fighting crime much easier.
It is the difficulty of identifying people on the Internet which makes it easier for crime.
Let's have more of your comments. Have a think about that, have a think about this question of where does the balance lie between privacy and fighting cybersecurity.
Before we take more questions from the floor, have we heard from any of our remote access commentators, people watching who want to comment?
Is there any comment from the remote access hubs on what we have been discussing?
He not yet.
Okay. More questions from the floor.
A gentleman here has been waiting a very long time.
If you could identify yourself so we know who you are.

>> Thank, Jonathan. I will speak in French.
My name is Jean-Jacques M. from Gabon, and I am a specialist in the area of ICT.
I work in Geneva.
Now, before defining the private and the public as far as developing countries are concerned, I would like to start by referring to some of the presentations of this morning and get to the specific with regard to cooperation.
Everybody talks about cooperation. What do they mean by cooperation? And what does it mean doing?
Everyone talks about it, the weakest link, but I think the weakest link is the poorest areas in developing countries, and all clients there are going to be using resources,

existing resources will be used in order for crimes to be committed.
So -- or to do something bad.
To refer to what was said earlier, this agenda which has been set up is fine. It's an excellent initiative. What we would like to hear now is what are organizations doing with regard to a specific agenda for cybersecurity. What's being done outside of these seminars for child security? UNESCO is doing something to help teachers who work with children in school, but what's Interpol doing in terms of the police? But what we are doing right here is setting up a coalition of networks, but we don't really know what the police are doing, for example.
So we have to work on security from the outset, and we have to work on resolving the problem.
We need to stop and think about these networks. What are the people outside the networks doing?
It's not today that we're going to invent something, but the universities involved in research, private laboratories are here, so we need to start the initiative again, pick up new tools. We talk about a lot of problems, but from the very outset, we need to put the security problem on the table. And then as the OECD said, the developed countries are working in different common economic areas and they can harmonize, they can pass legislation. But that's not going to stop cybercrime and promote security just because there's a law on the books.
Just because you have laws doesn't mean that you are going to stop cybercrime or promote security. But from the very beginning, you need to provide all kinds of different pillars of support. You need to provide law enforcement and legislative support.
So laws without law enforcement doesn't do very much good.
So you need to have training, then, for people involved in the legal system, so that law enforcement can take place appropriately.
Now we're asking people to be involved in these networks. We are trying to set up police for the network, but they have to be trained. It's a very specialized kind of knowledge that's required in order to provide policing of the networks.
Now we have the ITU has done this for the global agenda, but once this is done, you have to go one step further. As you said, you have to know what is the difference is between the public and the private. You have to discern the dinners.
Now you have talked about the Internet, but information is out there. It exists somewhere.
Once the information is published, it's out there.
Now, the person who is farming land is Gabon, in my country, is going to get a computer because he is told, well, with this computer you are going to be able to produce more bananas and more corn and he has to pay for that, 1,500 French CFAFs and he will spend 45 minutes cleaning up Spam and he doesn't even know what it is, so he is basically wasting money.
And then we are going to come and tell him that this is going to facilitate his trade or help him make a living? I don't know; it's sort of an unending cycle.
So the industrial business sector has to find technologies and solutions in terms of technologies.
And others have to stop cybercrime and promote cybersecurity.
Everybody has to work together: The users, those responsible for law enforcement, the technology producers. We have to work together, set up a network and have a collective effort to stop this.
Thank you.

>>JONATHAN CHARLES: The lady in front of you.

>> My name is (saying name), and I am from the association for progressive communications.
I would like to respond to the definition of cybersecurity, and offer a different -- maybe a different definition that has not come up. And also the issue of the balance and harmonization.
And I want to give you three examples where it does show that in some cases, while we talk of harmonization or we talk of different stakeholders, law enforcement, in some cases the law enforcers, in fact, may not be the best option.
For example, access to information. In situations where access to information is difficult, where there is political repression, for example, or where women are not able to access information in their countries but they are able to access information that is not allowed in their countries, now how do you -- is that part of what we are discussing here in relation to cybercrime?
In this instance, the person can be liable because of the loss of the national laws. But we were talking about earlier in the morning, for example, is that that does then is not -- contravenes freedom of expression.
My thinking is that we have an opportunity here to, in fact, use this to say that how do we use that to look at freedom of expression, expand freedom of expression because in places where that's not -- it's not all equal is, what I am saying, in terms of national laws that are in place. In some cases, it's repressive, and in some cases it is not allowed.
For example, people who use the Internet to network. People of different sexual orientation, who use the Internet to talk to each other. And what happens to them? They are persecuted because the laws in the country does not allow that.
Now, where does that fall in? How do we respond to that?
This is the only place that it's safe for them, where they find expression, where they are able to exercise their rights.
And they are exercising their rights in this space, and they are looking to international laws, they are looking at rights, international rights.
So where does that fall in in this discussion.
So in some cases, in fact, it's national governments and national laws that are repressive and are not helping.

>>JONATHAN CHARLES: All right. Let's put that idea out there.
There is the balance, isn't there? It is possible in tackling cybercrime that we are going to restrict our freedom of expression.
So where does the balance lie there? And how do you protect freedom of expression at the same time as you are tackling cybersecurity? I will come to Marilyn in a minute.
Gentleman there first.
And then Marilyn.

>>CASPER BOWDEN: Casper Bowden, chief privacy advisor for Microsoft in Europe.
I just wanted to address your question of the balance between cybersecurity and privacy.
It might seem obvious that this should be conceptualized as a question of balance and trading off one area against another, but this isn't necessarily so.
There are opportunities now with new cryptographic technologies to actually distinguish between the concept of identifying somebody and authenticating somebody to access a particular Internet resource.

The opportunity this creates is, in certain areas, to actually improve both privacy and cybersecurity.
It isn't necessarily a zero sum game.
And, in fact, I would --

>>JONATHAN CHARLES: Good to have an example. That's an interesting point. How?

>>CASPER BOWDEN: For example, in many situations that we have discussed over the past few days, we considered the question of child protection. But also, the preservation of freedom of expression for adults.
So the test is can you find a way of checking somebody's age? But on the other hand, actually distributing somebody's date of birth, that's extremely identifying information. It actually virtually identifies you in many circumstances.
So using some of these new technologies which I have referred to, and to give a plug, will be discussed further at a workshop tomorrow, 9:00 a.m., using these new technologies you can actually create a proveable assertion that somebody is over 21 or that they are under certain years of age.
Without allowing as it were the specific individual to be identified.
Now, these techniques are not perfect. In other words, there will always be real-world leaks and loopholes.
But using that idea of essentially proving one's membership of a group that is entitled to access some resource, but without necessarily specifically identifying the individual, I think we can make great improvements in both privacy and cybersecurity at the same time.

>>JONATHAN CHARLES: All right. Just to clarify that, though, they would presumably be identifiable to someone, the person who is verifying their age.

>>CASPER BOWDEN: Nope, not necessarily.

>>JONATHAN CHARLES: Okay. Right.
Marilyn, sorry, I promised you. I know who you are, but identify yourself to everyone else when you get a microphone.

>>MARILYN CADE: My name is Marilyn Cade. I am a private consult and have been involved in Internet governance issues now for some time.
I want to just comment on, if I might expand the definition of the debate we are focusing on by saying that, in my view, it isn't just balancing privacy and cybersecurity, but also balancing openness, balancing -- so we've talked a bit about freedom of information. But I think the issue of openness of the Internet, openness of the architecture of the Internet, that includes all those concepts that I think involve the ability of the individual to access information and resources they're interested in and also to be able to do so based on a choice they make. When they do that, they are in fact often putting themselves at risk.
And so I'd like to sort of expand the debate to say, you know, it's not just privacy or freedom of information, but also openness. And will we be driven by fear and by views that the perils of the Internet are so great that we are willing to sacrifice major benefits of this commitment to openness on the Internet? And that -- earlier, when you said what's your greatest fear, that's my greatest fear, because being afraid holds people back. Being naive keeps people at risk.
So I'll just say one final thing. I think that -- and I said this before in a conversation

that you and I had -- the greatest single threat to the Internet today is the user. The greatest single hope for the Internet is the user. But we have an uninformed user population. And we're about to add to it. We're about to add millions to billions of mobile users who are very used to a different environment and one where somebody else makes a lot of decisions for them.

>>JONATHAN CHARLES: So we're coming back to our education argument, aren't we, the need to educate. I think we'll look at that in a bit nor more detail in a few more minutes, because it's worth identifying in a minute. Alun Michael in a minute. Gentleman here and gentleman there. If you could identify yourself.

>>:First, I'm rather confused, because all the questions are being put at the same time, and it seems to me that there are some things that are working. Others work less well. And you approach things differently depending on one's perspective.
I would say that what works well -- and we could identify that. We did this morning -- the CERTs. They cooperate quite well amongst themselves, brilliantly. And they work in an anticipated manner.
You can also think of Interpol, which works well as well, in the area of protection against child pornography. And there are other areas of successful cooperation as well. So we've identified a number of different players that work successfully.
And as the OECD representative was saying earlier, states also have an important role to play.
I'm rather astonished that there's so little reference to the conference of the Council of Europe on cybercrime. It was, however, signed by Canada, the United States, and Australia, in addition to the European countries. This convention was signed. Now, that doesn't mean it was ratified. The problem of ratification always supposes that states assume responsibility for what they're doing.
But, still, here, we're dealing with cybercrime in terms of the definition provided by the Council of Europe. So that's the state role.
But I should say that in a forum like this one, what would be important, internationally speaking, would be for us to recognize the fact that there are tensions amongst us. Although they may not be crimes in and of themselves, phishing or other kinds of profiling, they're still -- even if they're not crimes, there's disagreement about them internationally. There are very different points of view from one country to another with regard to these ideas, phishing or profiling. And then there's the issue of spam, which is something that weighs down the Internet, but it continues to exist. And the same could be said with profiling. There's an upside and a downside.
Clearly, the Europeans have directives in place. But we also know how hard it is to obtain an agreement on travel safe harbor principles with the United States. And, in fact, as soon as President Bush got to power, he just let the whole thing go by the wayside.
Still, it continues to exist in the American mindset. But, still, their point of view is very different from the European point of view on this. If you talk about freedom of expression or other issues, all these issues are ones where we have different points of view. The European countries have an awareness about censorship, for example, which is quite different from how it's seen in the United States, for instance. So we need to look at some of the fundamental issues here. And we have to look at where can we negotiate with regard to this difference of cultures.
I think our forum is very interesting for that point of view, for negotiating in these areas where there are different points of view. Then there are other tensions, the tension between the business sector and society, for example, with regard to profiling

or spamming. They're both coming at it from a different point of view.
So I think, again, those are all areas where we could benefit greatly in this forum. So we need to start out by looking at what's working and what's not working and what are our different perspectives. Look at the various tensions.
Thank you.

>>JONATHAN CHARLES: The point you make on privacy is an interesting one.
Let me just ask you. We heard from the gentleman from Microsoft, who said -- how about that? -- we heard from the gentleman from Microsoft, who said that there wasn't necessarily a tension between improving security and privacy. We heard another view on privacy here, which is perhaps more European view on privacy compared to the American view.
I wonder how many of you in this audience -- and perhaps you'd like to comment on this -- agree with the gentleman from Microsoft that, actually, you can do both at the same time, you can improve security whilst not sacrificing privacy. Or do you see this as a tradeoff? Or is that a false question?
Alun Michael.

>>ALUN MICHAEL: I think it's very interesting that we're getting to this dichotomy and the tension.
I'm not sure that it's easy to find a way that completely reconciles privacy and safety. But I do think that's where we need to be recognizing that the tension is not going to go away. We're not going to be able to get a point where we recognize that.
What I want to argue for, having listened to some of the views that have been stated here, is to argue that the tension, the views that come from, on the one hand, the idea of complete freedom and keep the state out, and others saying, well, states have a responsibility, is the justification for the third way, if you like, or the IGF way of doing things.
I mean, frankly, it will be irresponsible to leave it simply to users. And the example that was given a few moments ago absolutely underlined that from a developing country point of view.
Nor can we leave it to governments. That way lies madness. Both have a role. But to pin the responsibility on either would be irresponsible.
Now, I underline again, there is a temptation to legislate. If you say there's a problem, and people say there ought to be a law against, it or the government is responsible, sore they'll bring in a law, laws rarely prevent what they forbid. And that is even more dangerous to try and seek it at an international level for two reasons. One is that we have to compromise all the views that exist right across different nations and different cultures and different levels of development. And, secondly, it will take so much time that whatever the danger was, it will be long past by the time we reach any legislation.
And the second point I would make is that many of the issues that we're debating here and that are debated in relation to the Internet are not really Internet issues.
So, for example, if somebody uses a footpath to reach my house and burgle it and steals things from it, that is not a footpath crime. The crime is the theft, the burglary. And similar with the Internet crimes, many things are not issues in terms of whether they're crimes or not. The issue is, can we make the Internet, the roadway, the pathway, if you like, a safer place to be by, for instance, improving lighting, which is known to increase safety in the physical world? So we need to look at those issues. We do need to have a necessary tension between rights and responsibilities. The tensions between freedom and law are not new. They're not unique to the Internet. They always exist in our debates in international contexts about where things should lie.

So I would simply argue that the IGF has to look for the third way, the way in which at a national level we balance the tension between freedom and responsibility, tackling crime, preventing crime, and all the rest of it, and that we have to use the IGF as a vehicle for inventing new forms of governance. And tackling crime is inevitably linked to the issues of governance. Who decides? How do we decide? And it needs to be faster, a more cooperative way of doing things that we invent. That's the challenge to us, not to decide which point on a spectrum we are going to settle on. Because we will be continually moving along that spectrum in relation to different issues.

>>JONATHAN CHARLES: So I just detect a little bit, Alun, that you think we might have to give a little bit on privacy to -- do I detect a little bit in your argument that we might have to give a bit on privacy, though?

>>ALUN MICHAEL: Yes, I don't think we can ever be absolutely safe from the dangers that are involved in the Internet, nor do I think that we can make privacy a total absolute. Neither of those things are tenable. What we have to do is to argue through the issues of privacy and safety and develop ideas of best practice, what is acceptable, and try to move forward together.
I know that sounds less efficient than having a decision or a convention or a piece of international -- I would suggest to you in the long term that it will be more engaged and actually more effective.

>>JONATHAN CHARLES: Sounds like an excellent piece of British pragmatism to me.
Gentleman here.
Can we get a microphone to the gentleman here.
If you could identify yourself and make your point, please.

>>RAUL ECHEBERRIA: Thank you very much. My name is Raul Echeberria. I'm the executive director of LACNIC.
I am tempted to speak in Spanish, but I think that people are not paying the same attention when the speakers speak another language different of English. So I will try to use my modest English here.
I think that there is a natural tension between rights and responsibility. But we cannot reopen the discussion about the universal human rights. This is something that has been discussed many, many years ago as trying to restrict the rights is a way to reopen the discussion about that. This is something that we cannot be tempted to do. And this is something that we have to avoid.
The tension, as I said before, is not between security and rights. The tension is between rights and responsibility. And it has been in this way for a long time.
So we have to be very careful. Because the bad news is not that we have to improve the safety, preserving the rights to privacy and freedom of expression. The bad news is that we have to improve all of them. We have to improve security and safety, but at the same time, we have to improve also the right -- the capacity of the people to exercise the right to privacy and freedom of expression, because thousands of -- millions of people in this world are living in conditions in which they cannot exercise the rights. And this is something that we have to warranty to them.
So I want to be clear, there is not a tension between the rights and security. The tension is between rights and responsibility.
Thank you.

>>JONATHAN CHARLES: Okay. Thank you.

Everton.

>>EVERTON LUCERO: Jonathan, this debate about -- and the tension about between privacy, security, and openness may take us for days, days or even years, we may debate that on how to solve.
I think that a more pragmatic approach, perhaps, would be to choose one specific subject that could enjoy a large acceptance, a subject against which nobody would pose any restriction that there is the need for action, for instance, combating child pornography. So on that particular issue -- and we should be issue-driven -- on that particular issue, should we prioritize the privacy? Security? Openness?
So I gave an example, but perhaps the audience would have others. And the second would be to try to get some inputs from developing countries. I think that is important to get their views as well on how they, with perhaps limited resources or perhaps lack of infrastructure or whatever, could also have other different challenges, challenges to the same problem.
Thank you.

>>JONATHAN CHARLES: Natasha, anything you want to say?

>>NATASHA PRIMO: Just a small point.
If we do take a particular example and we focus on child pornography, one of the points that came out of the second session that may be we want to pick up as well focused on the question of what is harmful content, what is harm, who defines it, who decides on what levels -- you know, what constitutes harm, et cetera.

>>JONATHAN CHARLES: Definitions are very difficult here. Maybe people are views on that. How do we define the issues that come into this whole debate on cybersecurity. What constitutes something that needs to be protected, that needs -- that we need to be protected from?
Bertrand. And then I want to call Senator Madrigal after that can we get a microphone down here somewhere.

>>BERTRAND DE LA CHAPELLE: Thank you.
First of all, I find the debate in itself incredibly interesting. And I'd like to make a couple of points on this subject, not on my personal behalf, but speaking here as a presidency of the European Union, because, basically, as you know, this is a matter that is of great concern and great interest for the European Union.
And, fundamentally, we do believe, and I think we strongly believe, in response to the questions before, that security, privacy, and openness can and should, in many cases, be pursued at the same time.
Of course, there will be cases where there are tradeoffs. And I like very much Raul Echeberria's comment saying that, fundamentally, it's not always a tradeoff between security and privacy. It can be between security and responsibility or rights and responsibilities.
The second thing is that if there is a domain where the interaction of all stakeholders is necessary, this is it. And there is a huge part of the work that is done by the private sector and the technical community. And we want to stress this as well.
But at the same time, in relation to the second panel this morning, it is very important to remember that we have all together, in all governments in the WSIS accepted a certain and reestablished a certain number of elements. And, in particular, I would like to recall the famous paragraph 42 of the Tunis Agenda that says measures undertaken

to ensure Internet stability and security to fight cybercrime, and to counter spam must protect and respect the provisions for privacy and freedom of expression that are contained in the relevant parts of the Universal Declaration of Human Rights and the Geneva declaration of principles. In this respect, we do believe that the rights and protections that are established by internationally agreed treaties and conventions are and should be fully applicable to the Internet.
It is a challenge. We all know it. But we have all signed it. It is important to remember that the documents in the WSIS contain a lot of the balance positions that we have discussed. And this message, in particular, was highly reaffirmed during a European dialogue on Internet governance that took place in Strasbourg a couple of weeks ago.
And I take the opportunity to make just one announcement, that the workshop that was supposed to discuss national and regional IGFs that were supposed to take place on Saturday will actually take place tomorrow morning in room six or seven in the first session, at 9:00. So as it was difficult to announce, it's important.
I just will finish with that, saying that for the European Union, the proactive measures are almost as important as the remediation measures, because it's a question of architecture. And as Alun Michael was mentioning, the question of lighting, sometimes the structure of the space can deter or prevent actions of a bad quality. And here I want to finish on a personal note.
Inasmuch as I appreciate what Marilyn was saying about the responsibility of the user, I hope we will not get into an environment whereby the equivalent from the real world would be, oh, I just simply walked in the street. I've been attacked by someone. It was my fault because I was not protecting myself. I mean, it's a general responsibility that the environment is trustable. And I think that Alun Michael was clearly showing from a parliamentarian view that the discussion we're having here is very close in its nature to the ones that all parliaments around the world have. And the fact is, we are testing here a very strange and new way to have that kind of discussion. And I must say that I'm very pleased at that stage about the interaction with -- among all the stakeholders here.

>>JONATHAN CHARLES: And I think that's one of the interesting things. Bertrand's raised the point, Alun Michael's raised the point. The interesting thing is, we are sitting here and thinking in some way we're in a vacuum. The Internet does not occupy a vacuum. It has a place in the real world, in real-world laws in different countries apply to it. Cybercrime comes under normal crime. There are things that can be pursued. And I think sometimes we forget that. We seem to think that cyberspace is something separate, and cybersecurity, and cybercrime are something different. Clearly, they're not. Maybe you disagree with me. Let me know if you do.
I want you to consider this issue of definition which Natasha raised. It is one of the issues. How do we decide what should be criminalized and what shouldn't? That's a cultural issue as much as anything. Something I think ought to be criminalized maybe some other country doesn't think should be criminalized. These are all issues. Let's have more comments from the floor. The gentleman over there and then the lady there.
Sir.

>>:Hello. As it was -- (saying name) from Hyderabad.
It was rightly pointed out in a big world, different laws exist. So it is very difficult to have a uniform solution regarding privacy and security. But I have something to say about accepting terms and conditions of a service provider.
I feel the terms and conditions are forced on the user by all the service providers. We

generally do not read most of the terms and conditions, but we accept, while giving our information, like, for example, creating e-mail or installing a new software, authorities, we give all our information, and we simply accepted the terms of conditions.
I feel there should be a governing body which will look into all the terms and conditions imposed by all the service providers so that it should not be one-sided.
I hope that is one important aspect.
Second thing is, who is benefiting from a crime? Let's say a user is the loser, basically. It is the company or the actual service provider who is getting the benefit. For example, antivirus company. I sign my laptop a virus and I am able to send a mail to the company providing the antivirus that the virus in my system is asking me to contact you. Why did you generate this virus on my system? He said, I'm sorry, it is not I have sent the virus to you. It is the reseller of my antivirus software has created this globally, and it is the reseller who is doing this.
Actually, and he has given up that he could not do anything regarding that aspect. He has not accepted the responsibility of his -- okay -- of his controlling the resellers.
I must feel that the service providers should take the responsibility. And since we are accepting all the terms and conditions of the service provider, we should have a governing body to look into all these terms and conditions, make them safe to the user also, the user point of view also to be taken care.
That's it.

>>JONATHAN CHARLES: All right. And maybe some service providers here would like to react to that. Put up your hands if you do, before we come to Liesyl, I think senator from Brazil has been waiting to make a comment.

>>:I'll speak slowly, since I'm speaking in Portuguese. And I'd like to thank the French interpreter as well for organizing this.

>>:Sir, there is simultaneous interpretation. There is simultaneous interpretation. You don't need to do it this way.

>>M.A. MADRIGAL: I am a senator from Brazil. And I am the chair of a parliamentary investigative committee. And we look at abuses against children. We investigate child pornography in Brazil.
We are talking about an ill which takes place in an asset of humanity. We will never be rid of the Internet. We will never be free of the Internet. Technology is advancing on a daily basis, and very quickly. But we need to understand that the Internet is not above good and bad. We're talking about something that's global and the great Internet operators, the big Internet operators throughout the world, like Google, which normally are providing services in their countries of origin, have to remember that the great drama here is that there's an arrogance. Countries that are developing, such as Brazil, they come to our countries, and they don't fulfill a social role, actually.
They come to our countries and provide a service, but they are servicing capital.
Now, that's not terrible. If they come to create jobs, that's a good thing.
But the problem is, they come to our countries and they say, "We are not going to abide by the laws in this country. Our company is based is America so we are going to abide by the laws of the United States," for example. And if the servers are in the developed countries, then we have two issues, two discussions. What happens with the developing countries?
It's necessary for the large Internet operators to understand and realize that it is a wonderful asset for the world, but they need to realize that it's necessary to abide by

the laws in which they are working.
Three years ago, Brazil was discussing the crime of child pornography in the public ministry with the federal police, with state level police, with other law enforcement, and people who go to congresses and conferences throughout the world.
And to me, there is a sadness, because in worldwide conferences, Internet discussions usually doesn't lead to anything substantial taking place in the country of origin.
So let's see.
We have a policy that's implemented in Brazil with the public ministry, and we have a parliamentary committee to investigate this. We have a judicial power. And Google was in Brazil and it had a certain behavior, because it didn't have to abide by our laws, even though we had them on the books.
They said that they were serving the disenfranchised.
Now we have to look at the other side of the Internet.
You have the human being. You have the child that's being abused, the family that's suffering.
And what we have to do is work with safe nets, safe Internets.
There are millions and millions and millions of children that get abused if nothing is done about this.
The people who use this system, there's a relationship page, there's a consumption.
Now this Google service is consumed in Brazil. It's the second largest in the world and a very large host. The other biggest host in the world is India besides Brazil for these services.
Now, as chairman of the parliamentary committee on investigating these crimes, I am calling upon Google to do something about this.
It's up to them. It's their choice to help Brazil fight crime, and especially to fight child pornography in Brazil.
They lied to us. They did not see.
I have used my judicial powers, and I convened them and I asked the federal police to go to the highest management of Google, that they should come to our country and face the justice system.
Now, on that day, we broke 3,274,000 child pornography sites, and another 20,000 with more than 10,000 child pornographers have been found who are circulating throughout the world on the Internet.
And in my hands I have child pornographers from around the world who then have to be turned over to the respective countries.
On the day that we seized these, the director of Google in Brazil, Dr. Alexander Hohagen, decided to do something about this in terms of justice in Brazil.
And so the large Internet operators need to do the same thing throughout the world. They need to allocate sanctions for this kind of behavior in countries throughout the world.
It's not possible to treat developing countries with arrogance. And that's why, today, here, I'm calling upon these countries, developing countries, to set up a coalition. And we need to sit across the table from the big Internet operators and talk about the role of Internet operators in each of our countries.
And we need to set up legislation in our countries to deal with this.
President Lula from Brazil just passed a law which criminalizes the profession of pornographic material from the Internet.
He also criminalized the conduct of child pornography for the person who looks at pictures of children who children in pornography. Anybody who facilitates this, who delivers it. A whole series of conduct related to child pornography has been criminalized.

This is to protect society, and each country should have laws on the books about this.
The Internet is great. It's marvelous. And as I said, we'll never be free of it. We'll never give it up.
But it is not beyond good and evil. And the operators themselves, nor the service providers, nor the Internet operators are above and beyond good and evil.
They need to obey the laws of the countries where they go to make financial profits and do business.
Brazil's experience, and this is happening right now, if we look at what Google Brazil is doing in order to promote the protection of our children, it's a good model.
These people, child pornographers, are around the world. And those who are working with us in Brazil in order to navigate the system and try and find these child pornographers, so they have to make it not just an Internet but a safenet for children.
The public ministry, the federal police and state-level police all work together with the parliament in order to do something about this problem.
However, for me, I'm sad to see that so few parliamentarians are dealing with this.
Because it's an instrument to defend society. And the laws are the main instrument to defend society, and they are voted on by parliamentarians.
And if parliamentarians are not visible, if they don't feel the same way we do, but if they refuse to see or because they refuse to feel. What we're talking about here is lifelong protection, protection of life, protection of the family, protection of children.
So the Internet, Internet operators and service providers, are much lesser than the interests of the family. And so it's necessary for everyone, each and everyone to obey the laws.

>>JONATHAN CHARLES: If anyone from Google wants to reply to that, I would be glad to give them the floor to respond to the Senator's comments. But again, it's a reminder a criminal act and a criminal act. Child pornography is a criminal act. It doesn't matter if it takes place on the Internet or somewhere else.
Again, we shouldn't be thinking in a vacuum about this.
We have a question our remote hub. We have people watching this in various parts of the world.
First of all, let me tell you we have heard from Monica A. in Argentina. She is watching us on the Internet and she says some people think that the solution for cybercrime and to increase cybersecurity is more regulation of the Internet. Others think that trying to regulate the Internet is like regulating the law of gravity to avoid access occurring.
What do people here think about these two positions and what do they think the IGF with contribute to make cybersecurity better and to fight cybercrime? That's a question for you to think about from Monica A.
And we have also heard, I think, from the Council of Europe who have sent in a statement from a remote hub, which we are not able to bring you right now, but they are also looking at us, are unable to be here at the moment.
More of your comments? Liesyl, I didn't take your comment, did I? You can make it now if you would like.

>>LIESYL FRANZ: Thank you again. My name is Liesyl Franz with the information technology association of America.
I just wanted to go back to the tension issue and reiterate some of the comments that were made earlier this morning. Because I think it's important to remember, and we have heard a couple of comments since I originally raised my hand, but that there is a mutually reinforcing dynamic between security efforts and privacy efforts as well. And I think it's important for us to remember that.

If you can configure tools, for example, for both, then that is the way to address the problem that is less about tension and more about mutually reinforcing efforts.
But it's also important to remember that it's not just technology tools that address both security and privacy. Organizations need to also put into place policies and procedures that we, as human beings in our daily life, for our job or whatever follow that -- again, reinforce what the technology tools with provide.
So it's a multidisciplinary and integrated approach to addressing both privacy and security.
I'd like to also build upon the comments that our U.K. member of parliament mentioned about the value of the IGF and what is of particular value about discussions like these.
We can hear about in a dynamic timely, topical way about ways that various constituencies from developing countries, developed countries, from civil society, from industry, from governments are dealing with these problems, and then take all of those aspects into consideration as we go back to our various posts and address them at home, and also, I would say, in an integrated global manner.
And I think it's the dynamism of the discussion that allows us to be topical with whatever the issue of the day is.
If we go down a regulatory path, just to address the woman from Argentina's question, then that can take years to develop and then implement. And by then, it will be irrelevant.
But we have seen over the course of the three Internet Governance Forums that we can, in a forum like this, address issues that are very topical, that are on top of mind for the participants, and relating to the issues of the day.
So I would just like to make that point.
Lastly, I just wanted to say that it's not always only individuals that are the victims or the losers in criminal activity. Companies do spend millions of dollars in trying to address attacks on their networks or extortion, which is one of the examples that was given earlier today about what are cybercrime examples.
And so -- but that has to be remembered as well, and we have to encourage an environment that allows them to also report those kinds of activities so that they can be addressed by law enforcement.
Thank you.

>>JONATHAN CHARLES: Thank you.
I want you to consider two questions now.
First question, I suppose, is the question of education. What can be done to educate? We have heard a lot here about the need to educate users. That's one way of tackling cybersecurity. How do we do that?
Some thoughts that you might have. I would love to hear from you about them.
And also, we haven't heard very much from companies about what they plan to do on this.
We heard a little bit from Microsoft of one example. But I just wonder whether anyone here from company service providers, who seem to be keeping very quiet on this issue, what they would like to say about some ideas that they have.
Before I do that, I would like to turn to another of our co-chairman who has turned up, that's Pavan Duggal who is an advocate of the Supreme Court of India, but also he is from cyberlaw.net. And I think you have probably got quite a few words to say on this.
This is an area of cybersecurity that is of particular interest to you.

>>PAVAN DUGGAL: Sure. Is this working?

>>JONATHAN CHARLES: You have to put it very close to your mouth to make it work.

>>PAVAN DUGGAL: I personally believe these are issues that the world really needs to have bigger perspectives.
Now, a large number of times we have been seeing that people are tending to do lip service. These are big linguals to talk about, but when it comes to hard core realities, somewhere down the line there is a lack of political will. The political will lacking is found much more in developing countries than developed countries.
The lack of political will is also because of the uninformed nature of the debate.
Now, invariably, people are looking forward to the top leadership in the west on how to tackle these issues. Now, it's historical reality that Internet got introduced, originated and developed in the U.S. and the west, but it's also a reality that the sun has shifted its focus.
The focus is now back on this part of the world where the developing countries, like China, like India and others, are going to basically hold fort. Primarily because of their size, primarily because of the Internet penetration, the depth.
In those scenarios, the culture values suddenly start playing a different ball game altogether. And it's here I personally believe that the concept of cybersecurity as a concept, as a way of life, is perhaps missing. To that extent, we can also see that in developing countries, even data protection, a concept of data as an asset is missing.
Now, it's far more important to create capacity building by the relevant governments within not only their own organizations but also within the netizen community, and also to transcend the digital divide to make people far more informed about what is cybersecurity, how can people contribute.
We have to appreciate, much that we would not want to talk about it, that there is a huge digital divide.
And even in countries like India there is a huge digital divide. How do you address them and how do you carry with you the huge chunk of people who are below the digital divide? For them, instances or issues like this have no relevance or bearing on their day-to-day economic survival conditions.
But at the same time, it's also important that the countries in this part of the world provide thought leadership. One way of giving thought leadership is to say hold on, this is a new legislation or this is a new approach that we are doing. Let's go about and propagate further.
Now, to give an example about cybercrime, now, internationally -- you just mentioned about an intervention by Council of Europe. Council of Europe has got its own treaty, the Convention on Cybercrime. A large number of developing countries, though, are in sync with the fact that the principles enshrined therein are extremely relevant in the context of this part of the world, but still do not have the political will to join them for a variety of reasons.
Similarly, when you talk of privacy, the concept is nonexistent in some jurisdictions, and the cultural and the social -- sociological factors are such that you can't expect a very kind of a uniform approach.
Let me give an example. You are here in India. India has got a law on information technology. It's known as Information Technology Act 2000, but still it's not very proficient or eloquent on the issue of privacy. Is the concept of privacy existing? Yes. But today when we are seeing more terror attacks, when terrorism is suddenly getting center stage attention, I believe the people here are willing to forgo portions of their privacy, just in a similar kind of manner as what happened in the United States. After the 9/11, people were willing to forgo their privacy for the larger good, being national

security.
Here also today, the systems are likely targets of attack.
It's bigger economies which are going to be dominant I.T. super powers, but are effective regulations, are effective mechanisms being involved? As a lawyer, as an attorney I have to say I am not satisfied primarily, because I have to look through the microscope. I have to look with a magnifying glass to find out hold on, what the country going to say on this issue?
Another big issue is on how do you ensure that the people have the adequate respect for privacy.
Now, in a country like India, it's still judge made law that defines what is privacy. The Supreme Court of India has defined that the right to privacy is a part of your fundamental right of life, which is guaranteed by the Indian constitution under Article 21. But yet there is no law of privacy in our country. So if you don't have a law of privacy, how are you thinking of expecting to implement specific provisions pertaining to protection and preservation of privacy of people in the context of Internet cyberspace, as also use of computers, computer systems and networks?
Another historical aspect that we need to consider is the fact that in these parts of the world, governments like to listen. If governments want to listen, electronic interception is the norm of the day.
Laws and legislations across different economies have detailed various legal mechanisms of how to effectively intercept. But are laws being followed? That's another major issue.
More importantly, where is the balance being made in this part of the world of, say, between developing countries, one on the issue of privacy and the other one on the issue of security.
I think there are huge challenges. Currently, I'm actually missing, as a proponent of cyber law, is the focus of political will to create more capacity building. That's one.
Number two, I want countries in this part of the world, the developing countries who are going to hold center stage attention on the Internet, to be far more focused in, number one, clarifying their vision and their strategy on how they want to deal with these issues.
Unfortunately, if you look at developing countries around the world, it's normally one legislation relating to Internet or computer systems or network. That one legislation is a jack-of-all-trades legislation. It will have, invariably -- it's like a typical Bollywood film. It has different elements of different drama, comedy, action and put together in one legislation.
I think it's time that the countries need to realize that these are serious, significant issues which require detailed, serious deliberations, specific provisions. And more importantly, I believe provisions which can actually be effectively implemented. This has to be supplemented by constant capacity building. Unfortunately, capacity building is one area that is lagging behind, to a large extent.
We need to ensure that capacity building has to be given the right focus.
And finally, I think at the end of the day, there is a need for updating. In the Indian culture you know we have a concept when you go back to the Ganges, which is a national river of India, it's a very pious river. You go back to the Ganges after a lifetime only to renew your energies, to dedicate yourself and your energies fresh. I think it's time that the countries of this world need to renew their vision on how to deal with these. Just because aspects of privacy are not present in your jurisdiction does not mean that the upcoming netizen population of your country aren't expecting privacy. They are expecting privacy. They are also expecting that you as nations are not only going to take care of their physical security but also the security of their data and

information in electronic form, as also the secure use of the computers, computer system and networks.
And if governments across the world fail in this scenario, clearly I think somewhere down the line a normal netizen has a feeling of deception. He gets a feeling of rejection and saying hold on, this is not what I was expecting from the governments. So that needs to be addressed.
And finally, I think somewhere down the line, you can't really address cybersecurity, you can't address privacy without addressing the much bigger issue of cybercrimes. Now, today in the Internet 2.0 world, people are vomiting on the Internet. When I say vomiting, people do not have the maturity of what they are talking on the Internet. So right from my girlfriend to my personal details to my past life to my hobbies. Hold on. Tomorrow, whatever you are saying is going to be indexed, is going to be archived for times immemorial and your children, your grandchildren are going to reference that.
So it's not a famous actress who is getting shot topless who is concerned her children are going to see it or not. It's now a question of you as normal netizens who are going to be impacted.
And if -- what happens if somebody high jackets my identity online? I am going to have a harrowing experience.
Now I have so much of a presence in different parts, somebody goes across and says I am so-and-so. Now, before I could know it, I am finished. Why? Because the damage that's caused is irreparable.
But are there legal structures, the legal regimes of the countries well equipped to deal with cybercrime? Not at all.
Why? Because cybercrime is considered as a hallowed sector somewhere on the horizon. Well, cybercrime can never touch you.
That kind of a vision needs to go out. The ostrich attitude needs to give way to far more pragmatic thought process. Hold on. Cybercrime today is a part of the developing countries. India, and this morning in one of the sessions I was informed, is at number nine of the total number of the top ten countries from where spamming is being originated. Number one still being the United States.
Well, vernacular content has really ensured that vernacular Spam is now coming.
Now, in India we have come up with the concept of voice SMSs. Rather than sending your SMS to your mobile phone, I can leave a voice mail for you. Hold on. People leaving all kinds of voice messages for you on the Internet for other people to download, listen to you? I am actually seeing a scenario which is going to be a horror kind of a scenario for individuals, for management of Internet reputations. But more importantly, for trying to protect your national computers, computer systems and networks.
There's a concept known as the protected systems concept, which is that certain governments have reserved upon themselves the rights to dedicate certain critical infrastructure as protected systems. And if you are trying to merely have access to that protected system, that access has been defined as a penal offense punishable with a high quantum of imprisonment, say, ten years' imprisonment in India, and fine. This is one mechanism which countries can effectively utilize to go ahead and dedicate not just your critical infrastructure, but also normal, regular computer systems which have a bearing upon not just the stability of your national Internet exchange, but also upon the deliverance of electronic governance functions in a manner that it reaches the common man. So I think it has to be a variety of approaches. Merely lip service is not going to do. Today, the netizen is an extremely disappointed and yet a very angry lot. The recent Mumbai attacks have shown, hold on, the people of India are coming on the

streets and saying, we want accountability, and enough is enough. And mind you, enough of that propaganda or shall I say the anger is actually being vomited through the Internet. It's time that the national governments try to find out how can they effectively deal with it, how can they effectively secure the computers, computer systems, the networks, how can they actually come up and constantly upgrade their criminal regimes and the legislations in such a manner so that the latest and the new kinds of evolving cybercrimes are effectively covered, and yet, at the same time, still have respect for individual rights, have respect for privacy. Just because, well, the country's under terror attack does not mean that you have a certificate blanket license to go ahead and intrude upon any computer record of any computer system. Mind you, let me give an example of India. In India today, Indians still like to save their personal details, their personal on Web e-mails and e-mail accounts which are free e-mail-based accounts. So I think it has to be a cumulative kind of approach. It has to be balanced. But far, far more important is the commitment, the reiteration of political will to ensure that an adequate balance is appropriately arrived at not only between cybersecurity and privacy, but also at any other aspect which tends to impact negatively or injuriously the effects of interests of people who are using computers, computer systems, computer networks, as also data in the electronic forum.

>>JONATHAN CHARLES: Thank you very much, indeed. And I think a very interesting point there where there are obviously circumstances where people are willing to sacrifice privacy for a better overall daily experience, whether it be with the Internet or their personal security, but in this area of cybersecurity, maybe people are willing to make that sacrifice.
We've got about 40 minutes or so left to go. We've had another question from Myra (saying name) access hub in Argentina, who says she's really drawing attention to this whole issue of definition, defining a crime, which is crucial for cybersecurity.
And she says, is holding a pornographic photo for personal consumption a crime? That's one of the questions. Or only those cases where the photos are used for commercial purposes? So, for example, would it be criminal to hold a pornographic photo for your private use?
That's a comment she made, actually, after hearing our Brazilian colleague, the senator, talking about the issue of child pornography in Brazil and how to they've cracked down. So, again, question of definition is what she's asking. I put out the question a minute ago about education, about where we start on that. And also Internet service providers and other commercial companies about where the responsibility lies with them.
And I'd like to hear your views on that now. And I'd also like to you consider one other question, which is something that occurred to me a bit earlier on. One thing we all love about the Internet it its dynamism. That's been the Hallmark of the Internet for the past few years, a very dynamic environment.
If we make cybersecurity the number one issue, are we affecting the dynamism of the Internet?
I don't know.
Anyway, your points now. Put up your hands, and I'd love to hear from you. Lady there. Yes. If you could say who you are, that would be great.

>>:Yeah. My name is (saying name) and I am from Russia.

>>JONATHAN CHARLES: If you could hold the microphone and say it again and hold the microphone up to your -- yeah. You have to hold it quite close to your mouth. So

--

>>:Is it okay?

>>JONATHAN CHARLES: That's better.

>>:Okay. My name is (saying name) and I am child protection activist from Russia.
As child protection, I see how effective the framework convention on tobacco control is. And it is effective partly because it's convention of the United Nations.
Cybercrime, and especially child pornography, is a huge problem. However, because it's been unresolved, it's taken a disproportional amount of time, I would say. We have convention of the Council of Europe, which -- and it has its benefits and its limitations. Benefits, this is a group of countries with great expertise. And limitations is because, basically, not all countries are ready to take these approaches.
For example, Russian authorities, they cannot take these approaches which are good for the European Union. So what I would suggest is to consider the idea of develop some kind of working group, some kind of work thinking how could we either integrate child pornography into the existing treaties on the United Nations level or to develop a new treaty. Maybe it's a bit revolutionary, but I think it could be -- the time could be coming soon.
Thank you.

>>JONATHAN CHARLES: All right. Thank you very much.
Lady --

>>:Hello, hello.

>>:Hi. I'm (saying name) from Bangalore, India.
I'm sorry, I'm not an ISP. So I think this is going to be one forum where the users take over and the companies are not talking. Yay for us.
And I just wanted to talk about, as mentioned already, it seems like child pornography is taking a disproportionate amount of our energy and effort. But just to add one more thing, especially in relation to John Carr's presentation in the morning as well, that there has to be a way to talk about children and protection of children while also taking into account that their sexuality also has to be talked about and they have to be given a space, safe space, within which that can be explored. Children are not necessarily nonsexual beings. We seem to have a lot of rhetoric about childhood premised on the idea that childhood is about innocence and that there should be paternalistic protection. I think we need to look at that a little bit more carefully before going on and on about it.
I also think that the disproportionate amount of energy might be because there are ways in which women or anyone marginalized, maybe even developing countries can participate in processes like this, and we get pigeonholed into topics like child pornography or into issues that are not necessarily allowing us to speak directly on national security, on cybersecurity, on cybercrime. And so there are ways in which a person like me can only intervene in certain -- on certain issues.
So I think that might be an explanation why certain amount of disproportionate energy is being devoted to something like this.

>>JONATHAN CHARLES: Thank you very much.
I think Thomas Schneider over there. Yes, get a microphone to -- yep.

>>THOMAS SCHNEIDER: Hello. Do you hear me? Yes. My name is Thomas Schneider. I work for the Swiss operator for media and telecommunications. And I work quite a lot as a member, a state representative, at the Council of Europe. At the moment, I am chairing the expert group on human rights and information society. And due to the absence of the Council of Europe, I might be one of the few who can bring in a little bit of the work that we are doing.

And just to answer a few things that have been said, the Council of Europe does a lot of work in protecting the rights and freedoms, apart from cybercrime, but rights and freedoms of citizens, like freedom of expression, privacy, and other rights. And in the group that I'm chairing, we decided to -- apart from using the traditional mechanisms, like recommending member states to do this and that and to take care of this and that, that we have started to contact the industry directly. We have tried to identify what are the key actors in the information society in the Internet that have a role with regard to the human rights of the citizens of the users, with regard to the freedom of expression, with regard to their privacy. And we have realized that many industry actors are in a different situation because there are certain expectations or different expectations to them from law enforcement agencies, but also from a human rights point of view, that they are sometimes, and especially the ISPs, squeezed into a situation where they themselves have an interest in having a clearer view on what their roles and responsibilities are and also what the limits of their responsibilities are.

And we have engaged into cooperation, for instance, with the European Internet service providers, and we have elaborated jointly with them guidelines that help the ISPs to be more aware of the effects of their work with regard to the human rights and also including privacy and freedom of expression of their customers, of their client and how they can empower their own staff, people who are dealing -- people who are working for ISPs, how to help the small ISPs that maybe are not -- do not have the resources to follow meetings like an IGF and so on. We have engaged in working out guidelines for the gaming industry, the European gaming industry, close contacts also with Microsoft, who is very active in that field, that we try to raise awareness with those who create the games, those who design the games, that they should be aware of the effect that their games can have and how they could follow kind of human rights standards if they want, because it's voluntary guidelines. But at least the willingness of the gaming industry is quite high, because they fear, of course, if they do not give themselves some standards, that it might be lost, it might prohibit certain kinds of games and so on. So there is an interest from both sides in self-regulatory mechanisms that work. And whether they work or not remains to see. We presented these guidelines in October this year.

There's more work that we plan to do in this field. We are also thinking about -- and there was a workshop this morning on the governance of gatekeepers, on those mainly private sector actors who are not media, but who shape the access to content, and of search engines, if you take the example of search engines and privacy, there are search engines that have code of conduct with regard that they store your data only for two days. Others do not have such kind of things. And if the willingness is there on behalf of the search engines, we would be ready to work with them to help them set up kind of a set of voluntary principles which they can adhere to in order to help the user find out where his privacy is better protected. This is just one example.

And for all those who care about the identity and privacy and dignity of -- the dignity of identity and of children, but not only of children, there is a workshop on Saturday morning. It was initiated by the Council of Europe, and a few people are now carrying this initiative forward, on expression and image and identity online. This was

workshop number 18 that was scheduled for tomorrow. And we are now merging this with the workshop 32 in the time slot of the workshop 32 about the security, dignity, and privacy of children in the online world.
So you're very much invited to join this.

>>JONATHAN CHARLES: Thomas, thank you, indeed. And you've mentioned the Council of Europe. We've had a couple of questions. The first was from the Council of Europe. Who was unable to be here, but they are watching this. This is a question from Alexander Seger, from Strasbourg in France. He said at the Council of Europe level, there are a number of adopted guidelines and treaties that show it is, indeed, possible to square the circle and maybe security, privacy, and openness not only compatible, but mutually reinforcing goals. These include the Convention on Cybercrime, as a global guideline, human rights guidelines for ISPs, openness benchmarks with regard to the public value of the Internet, freedom of expression and Internet filters, as well as regarding the protection of the security, privacy, and dignity of children on the Internet.
These may also be useful, he says, for societies outside Europe.
And a related comment or question from another remote participant asks if the ITU cybersecurity agenda and its model kit on cybercrime will be a competing or supplemental instrument to the Council of Europe cybercrime convention. And they'd like to know, what do the IGF participants think about both the convention and the ITU's cybersecurity agenda.
Your comments where we're going to go next. Let's go there, yes, lady in the -- just there, yep. We'll get you a microphone. Yes, you.
And then we'll go to the gentleman in front of you.

>>:I can be heard?
Okay. I am Anita Telefrancia (phonetic) from the group, the (saying name) association. We are involved in the field of education and culture. So I would like to make a remark about what was asked a while ago about education.
Education for the Internet or for that matter, any other objective, I would put it in the context of education as a whole, which means that today, I think the world is in need of quality education. And we can even see that in the actual Internet. If you see, for example, the number of Web sites dedicated to interactive, reflective Web sites, I can say that very few are available. And also, that even in terms of networking, social networking, even precedes, or it's even higher, there are more people going to social networking rather than to networking for reflection, having common ideas, putting ideas together.
So I think there's a crisis there.
And I would say that education for Internet will not be just the punctual thing of education for Internet, but, rather, I question education today. Because education today is just like a stepping-stone towards economic liberation or economic stability, but it is not real education in the sense of giving or equipping the person to develop the potential to the full and making use of his or her talents for integral development and for transformation of society. That is what I call education. And that is important for us to know that education today is beyond the classrooms.
So all of us who are gathered here, adults, we all have this responsibility of educating in the family, in the workplace, even here among us. And education also has this important aspect of witness, of testimony. So even how much you tell a person, a small child, but if you yourself don't live up to the ideals, then it's of no use. And, therefore, to me, it cannot be taken out of context. To me, it's quality education right

now, and even in our schools, everywhere we are.

>>JONATHAN CHARLES: All right. Thank you very much.
If you could just give the gentleman that microphone. And then after that, gentleman here.

>>HITESH BAROT: Thank you, Jonathan. My name is Pavan Duggal, from Cyberlaw. And for Web 2.0 users, for history, I would like my thoughts to be recorded as Pavan Duggal.
So the question is, is it this microphone's fault for not checking to see whether I was Pavan Duggal? Or is it IGF's fault for allowing me to represent myself as Pavan Duggal? Or is it the translator's fault?
There are so many levels on which it is -- A, it is me committing the identity theft. However, there are a number of pathways or footpaths upon which this burglar entered the house. And we wonder how many of those people we can hold responsible for my action.
So I'm glad you indulged me with that. Looking at me. Crazy.
My point, reflecting on the European Council's message that you just read to us about the ability for openness, security, and privacy to all coexist, without necessarily having tradeoffs, I think that's something that's definitely possible. In fact, we heard earlier today, I think it was in the first session, where the comment was made that although privacy is a lot more cultural and needs to be respected on more of a local level, security can be a lot more objective and can exist with a certain set of common ideals and principles that could be -- and then the word introduced by (saying name) was -- interoperable. So if there are some regular standards that everyone can agree to that are more subject- -- that are nor -- not subjective, that are more objective. And then the privacy aspect has come in with some more cultural context. And it's very possible within a framework of interoperability to have all these goals be met without necessarily doing a tradeoff.
One might say, you know, prolonging the analogy before, is, would, then, IGF be responsible to checking the frequency of my modulation of my voice or my DNA and figuring out whether I was Pavan, and then, therefore, did they violate my privacy in doing so. Do I have the right to be anonymous or to pose as someone else or do I not have that right? It's a sticky question, obviously, which is why it's not going to be solved today or in the near future. But certainly one step that I think -- it may not be the appropriate time to talk about this right now. But one step is the fact that we're here in this room having this dialogue and the different stakeholders are expressing their views. And then when we do go back off to our posts -- at this point, I'll mention that my name is Hitesh, and I work at Intel. When we go back to our posts, we take some of the learnings here and try to implement them, with innovation, like the colleague at Microsoft spoke about. There is going to be innovation that is going to make it possible to both be -- have cybersecurity without the risk of the privacy of the individual. And that's stuff that's happening right now as we speak. And that's, I think, ultimately what's going to be the solution, is innovative solutions, some of them springing forth from the dialogue we have here today.

>>JONATHAN CHARLES: All right. Perhaps I should say, (saying name), thank you very much. Or maybe Pavan Duggal 2.0. Thank you.
The gentleman there has been waiting quite a while. Can we get a microphone over here.

>>MARTIN BOYLE: Hello, my name --

>>JONATHAN CHARLES: We can't hear you. Maybe the microphone will have to be slightly closer to you.

>>MARTIN BOYLE: Hello. Right. My name is Martin Boyle. And I failed the first test of being able to turn the microphone on.
I am at Nominet, which is the dot UK domain name registry. And I'd like to pick up on the point of industry taking responsibility for trying to improve the security for general people using the Internet. We're not an ISP, but we have membership that includes Internet service providers and registrars. And I'd like to just choose through examples of how we are engaging with that community and with others to try and achieve that objective.
The first is in a dialogue that we've just started with the banking community, where what we are hoping to do is to start sharing information about the sorts of phishing attacks that the individual banks are starting to see and then trying to identify whether there is a way in which our members can react more quickly for taking a phishing attack down, bearing in mind that most of the damage in a phishing attack happens within the first few hours, and, therefore, if it takes you 24 hours to take the site down, then it's rather too late.
So this is the industry reaching out well beyond its normal community to try and achieve something that is rather more effective.
The second I'd like to mention is the Internet Watch Foundation, where we and, in fact, the Internet service providers in the U.K. are all members of this industry-led organization which seeks to address child abuse and hosting of child abuse on U.K. sites and to try and block access to sites that are actually illegal for access within the U.K.
Now, the Internet Watch Foundation is currently working on its way of addressing what is currently called extreme pornography, again, something that is against the law, and, again, an area where we are going to have to try and examine ways of responding and trying to protect people from this nature of material.
And the third is that Nominet itself has set up a charitable foundation. And one of the roles of the charitable foundation is education. And this is picking up the point that was made earlier that we would hope that the foundation will be able to fund initiatives that help improve people's awareness and experience of being able to identify and respond to the attacks that affect them.
Thank you.

>>JONATHAN CHARLES: Thank you very much.
Question, a written question, we've had from Sophia (saying name) director of telecom, who says all the discussions so far are going around a few examples, for example, what we're really discussing is trust in digital life, which is context-based to make the cyber world secure, open, and privacy protected, with responsibility and accountability. And how do we develop trust in digital life?
That's the key point, I suppose, here. It is all about trust. The Internet requires trust to work. I was suggesting earlier, actually, it's better to have no trust, because then you're not complacent. If you go into the Internet completely trusting, well, you're complacent. If you use the Internet as a user not trusting, maybe that's better, you're more aware of the dangers out there. But it does relate to this issue of trust.
In our next few minutes -- we haven't got many minutes left, about another five or so minutes of discussion -- can we also consider the issue of what we're all doing here,

the IGF, and whether there's a role. We've heard quite a few people here say maybe there is a role for some sort of cooperation between all the different aspects, the users, the companies, governments. Is that where the IGF comes in? And if so, how? Question -- I'd be delighted to hear your comments on that, as well as our other issues as to what else needs to be done.
Okay, gentleman here. You put up your hand very swiftly.

>>David Appasamy: Good evening. I'm David Appasamy, from Sufi Technologies, which is a service provider.

>>JONATHAN CHARLES: Good.

>>DAVID APPASAMY: Okay. I couldn't agree more with what Pavan had to say, or what we're discussing here. I can assure you that, as a service provider, we welcome measures or cybersecurity that worked and were practical and which facilitate greater use of the Internet.
Coming to the question that you were talking about, what is it that we can do here at the IGF, one problem that we are all aware of but doesn't usually get addressed because there is no global convention to deal with it, is spam. The fact of it is, 80% of the traffic over the Internet is spam. And we're all paying for it. All the bandwidth providers, all the service providers, 80% of its capacity is choked by this, paying for its transmission.
If, using a platform like the IGF, you could have a global convention that would shut down the servers from which spam emanates or whatever, I mean, we need to discuss it. I'm not providing solutions here. It would be of tremendous service to the networks around the world and to people in general. That's one.
The second point I'd like to make is the problem that Pavan posed in terms of developing markets and the political will to do something about it.
I'd like to add to that, it's not just the political will. Often the people who are deciding policy, they don't use the Internet. Many of them don't use computers. So they don't really understand what the issues are. And it can be as simplistic as if something goes over a network, the person who is operating the network is culpable and goes into prison. But if a terrorist goes down the road, you don't shut down the road.
So that is a huge problem.
And I'm glad my friend stood up and made those points in terms of the nuances we need to consider. These are things that need to get discussed. And I think we need a certain level of maturity and understanding to be able to come to a workable solution on cybersecurity. But I can assure you that service providers will be at the forefront of it. Thank you.

>>JONATHAN CHARLES: Thank you very much, indeed. And the lady I kept waiting.

>>:Hello. This is (saying name). I'm an instructor at (saying name) university faculty of law at Ankara, Turkey. I'm also an ambassador here. But these are my personal views.

>>JONATHAN CHARLES: If you can make sure you hold the microphone very close to your mouth. Okay.

>>:Okay.
I believe while preventing cybercrimes, the role of effective data protection is also crucial and should not be underestimated, because it will prevent many of the

cybercrimes, especially with the financial ones and the privacy-related ones. And I think it's preferable rather than rushing into imposing criminal sanctions.
With regard to the definition problem of content-related cybercrimes, yes, this is a problem. We might have the same titles, take defamation, for example, many jurisdictions has that, or obscenity. But if we say define obscenity, are we going to take sexual content or are we going to consider violent content, either? This is a question. And each jurisdiction has its own value judgments based on cultural and historical experiences.
The only consensus seems to be in the prevention of child pornography. But even there, if I ask, what is the definition of a child, or if I ask, how are you going to treat adults appearing as children? Again, we might have many, many different answers.
Apart from that, with regard to education, I think the education should not only be limited to the users, but also to the policymakers, members of the judiciary, because their roles are really crucial in the whole process. If we are ever to regulate cybercrimes, I think we should choose effective sanctions. With regard to content-related cybercrimes, the general sanction followed by many governments is to block access to Web content, which is a hot topic in my home country, too.
But I think in many cases, this will be ineffective, as the blocking access order is mainly based on I.P. addresses, and with simply a change of your proxies, you can easily avoid it, which will remain the sanctions ineffective.
Thank you very much.

>>JONATHAN CHARLES: Thank you very much.
How are we doing? Okay, probably time for a couple of more interventions.
Yes. Marilyn.

>>MARILYN CADE: So the question, I think, is, what are we doing here in the IGF that has value and is going to make a difference about cybersecurity, openness, et cetera.
I don't think that, actually, this is the place to negotiate global agreements, but I think it is definitely the place to build better global understanding. And I'm just going to say, as somebody who works in intergovernmental organizations by participating in them, who goes to a lot of different places, this is the most unique forum that I see, and one of the unique aspects of it is it's maturing. And people are beginning to talk about topics that, two years ago and one year ago, they weren't really willing to talk about. They didn't have enough trust in each other or in the forum to bring forward topics where there was great disagreement.
So even the fact that we are dealing with these topics that are very divisive and involve different understandings and different roles I think has a great value.
I think we already learned a lot today from each other, and so I would say this idea of really deepening the understanding across the different players, but also across the different geographies, it's bringing a lot of value, and may better inform decisions we make in other settings and back at the national level as well.

>>JONATHAN CHARLES: Okay. Thank you, Marilyn.
I am going to give three people one minute each. So lady with her hand up there, Bertrand and the lid did I here.
Yes.

>> Hi. I am (saying name) from Bangalore, India.

>>JONATHAN CHARLES: Make sure you hold the microphone up to your mouth.

>> I think this is the third or fourth year -- third year of the IGF, and I think I was there in the first year, and it's a bit -- I mean, I don't necessarily see that there has been that much progress. In fact, this year seems a little duller than before, but maybe that's one of the reasons --

>>JONATHAN CHARLES: I'm sorry about that. I have done my best.

>> You are trying.
Anyway, the one thing that I would like the IGF to look at would be that a lot of conversations around access for all need to be also about protecting current ways in which people access the Internet. Instead of necessarily replacing those and looking entirely at government-led ways in which access can happen, which is really important in the rural Indian context because only the government can go into the villages. But there are these ways in which there's what we call the cyber cafe revolution in the cities of India, which is how ordinary people access the Internet at ten rupees an hour, which is remarkable. But that is slowly being wiped away.
And these are small businesses which maybe is something that should also be looked at. How do we access the Internet now? Can we protect those ways instead of necessarily always looking for government ways in which to replace it.
The second thing I would like to raise is about protecting children, which comes up again and again, and about how children need to be protected from harmful content. And I would just like to remind that there is the convention on the rights of the child that says anything that has to be done for children has to be in the best interests of the child. So again reiterating that children have a wide variety of experiences and all those need to be taken into account.
The last thing is that we often talk about censorship across different jurisdictions, across different legislations.
We need to nuance this. There are ways in which there is pre-censorship, which is continuous filtering that the ISPs might do in terms of, say, extreme violence or extreme pornography, war pornography, et cetera, which is continuous filtering, and there is also stuff you put out there, like books are put out there and then someone complains about it and then it has to be withdrawn.
So when we talk about filtering and censorship, one has to note that in developing countries especially, like in India, it is always complaint led. Someone complains about a Web site, it is then withdrawn for a limited period of time. It then comes back. There are also other examples of continuous filtering, which the two need to be separated from each other, especially when one needs to look at healthy public discourse where unpopular speech is as important as popular speech.

>>JONATHAN CHARLES: Thank you.
Bertrand. Can we have a microphone over here? I will take the gentleman over there in a minute but not yet.
Hold on, just wait your turn. I will be right with you.
Bertrand wanted to make a comment first. Microphone here.
Don't worry, I haven't forgotten you.

>>BERTRAND DE LA CHAPELLE: Just one very quick point to note, and it's on a personal basis.
The expression that was used that child pornography is taking too much of our time at the IGF, I think actually we should take this as a signal of maturity.

This issue has reached a certain level of awareness, diversity of perspectives in the last two IGFs that we are now moving to another layer, which is what are the tools, what is the approach, and what are the places where this must be discussed.
I don't think it is the subject, anymore, of large debates, and maybe in the next IGF some of the workshops that have been working separately should really get together, build -- even in between, on what has been discussed in the two previous IGFs and maybe come to the next one to discuss various proposals, involve other actors and the various formats that could be thought of.
There may be conventions that I am not aware of that could be complemented. There probably are different frameworks that exist that should be articulated.
I personally don't know the details, and I think the next step is now that this issue is clearly accepted by everybody as a very important test case, is to see how it can be explored further.
Not treated and solved at the IGF, but moved one step further.

>>JONATHAN CHARLES: Thank you very much.
Lady here I promised, and then I will go to the gentleman there I promise you, but I did promise this lady first.

>> I think -- My name is Chad Garcia. I am from APC.
In relation to what other things can be done, I think is to also, to add on to what the lady here is saying, is the maturity actually should also include inviting others who are not here.
And I think there are others who are not here with us. For example, that will enrich the discussion around, let us say, how the Internet, protection of women, protection of women in terms of violence, violent content, harmful content. In that discussion there are people -- there are organizations, there are conventions, in fact, that we need to also look at to expand the discussion of rights.
And I think, just to add to what Bertrand is saying, that needs to come into the discussion because there is a whole world that is not included in this discussion.

>>JONATHAN CHARLES: Thank you very much.
Gentleman from China. Yes.
Yes, yes.
Have you got a microphone? No. We will get you one, don't worry.
No, no, the gentleman over there is -- yeah.
The gentleman with his hand up there from China.
Thank you.

>> I still prefer to speak in Chinese.
I come from China. I am the Secretary-General of the Internet Association. My name is (saying name).
I run into a problem in my work. That is many people mentioned the issue of protection of children to prevent child pornography on the Internet.
In China, in adult Web site, it is not allowed to post such things. It is illegal to do so. But in western countries, in many other developed countries, in many Web sites for adults, we do see this kind of problem.
We have some statistics that is in the states, for the moment, there are about 1 million Web sites that profit out of this would be about $40 billion. In China, it is not allowed to have these kind of pornographic Web sites.
We do have organizations like SBU which would block these Web sites. And the result

is, in those western countries, they are making a lot of profits. The more profits they make, then the higher the cost for us in China.
Therefore, I suggest maybe we can do something here. Here in IGF we have always been talking about how to respect diversity and I am wondering in the future, how will this issue be resolved?
Maybe we can use this forum to deal with the issue.
Here, I'm just raising the question. Thank you.

>>JONATHAN CHARLES: Thank you for waiting.

>> I just have a small point.

>>JONATHAN CHARLES: Very swiftly.

>> I am the chair on the faculty of university of (saying name) University, India.
We are talking so much about the child pornography and cybercrime, thinking that there is a lot of awareness in the society, but the hard reality is that, you know, I have done the research on 1500 people including children, parents, and the teachers, and very, very little awareness about the cybercrime among the teachers.
And the most important thing I would like to make a point here is that we can't keep the developed countries and developing countries on the same platform.
Maybe we can have a global understanding but then we need to work out the specific strategies to the developing countries.
And I think we need to empower the different sectors in the Internet, like children, parents, and look at the digital divide in the country.
I think we need to address here, is I what want to make the point.

>>JONATHAN CHARLES: I will take one very quick 30-second comment because the lady is very persistent hereon the left-hand side.

>> I want to say that we should discuss in the Internet Governance Forum is the different approaches to the definition and (inaudible) of cybercrime and the ways how to harmonize these different approaches.
And so only about 30 countries has ratified the convention of (inaudible) crime, and there are a great variety of definitions of child pornography among the countries which haven't ratified this convention.
For instance, in Russia, there is no judicial definition of child pornography, and so there is a great problem for us.
I think I would like to support these initiatives to develop the treaty only be a protocol on cybercrime and especially on child pornography which can unify and can criminalize the different approaches to cybercrime and especially the child pornography.
Thank you.

>>JONATHAN CHARLES: Thank you very much.
Everton and Natasha you have been listening to this. Give us your thoughts now.

>>NATASHA PRIMO: Well, I will give what I saw as the issues that had a lot of traction, and some of the consensus, I suppose, that has emerged through the debate.
Three or four points, really.
One is that there seems to be an emerging consensus that this is the issue of dealing with cybercrime, cybersecurity, privacy and openness is a joint responsibility; that we

should rather look at roles and responsibilities of the different stakeholders, and look at it as people working in -- synergistically.
There is a definite need, through the discussion that's emerged for more information about where to go. So who to turn to in the case of people becoming victims of cybercrimes and trying to find a remedy or process in the off-line or real-world environment.
And this was said while noting that there was some talk around the role of enforcement, and the point was made that in some cases, going to enforcement officers, to law enforcement officers, may not be the best root because they may be, in some cases, also part of the problem rather than the solution.
And here the reference was specifically to repressive states.
There was also recognition that there is, in fact, a lot happening, but that we need, as I said earlier, a discussion about how these different stakeholders would interact with each other to resolve incidents.
Okay. The second point that I suppose also relates to this is that it's not necessarily -- we shouldn't necessarily talk about a tension between security and privacy, but that these can be mutually reinforcing. And also picking up on the point by Marilyn Cade that we need to also, as part of this discussion, bring in the implications for openness.
Further to that, that the tension should be reconceptualized as that between rights and responsibilities, and this also brings into focus the importance of education, and specifically media literacy for users.
Another view is that -- oh, what I just said, I suppose, is it's less a tension than about mutually reinforcing imperatives; i.e., security, privacy and openness.
Just quick around the role of the IGF, I think people feel very positive that it is a space for developing consensus, for developing deeper understanding of the different viewpoints, the different perspectives, and that this has value in and of itself.
And there was some skepticism about whether we could reach a decision here, but this is the consensus and the deep understanding may lead to better decisions, more informed decisions in other spaces.
And just finally, then, on the child pornography issue. There's been a number of points made by different people about this perhaps not being the appropriate space to take up this discussion any further, and that we need to move to look at mechanisms, measures, processes, and difference in other spaces, more appropriate spaces where the issue can be addressed more effectively.
But it's also raised the issue for the need for a more nuanced debate, that people have thrown up the question about what is a child, what is harm, what is harmful content.
And further to that, that there are people who or stakeholders in this discussion who are not part of the debate here who, as we move it forward into whatever spaces we take it, that we also need to bring those communities, those interested parties into the discussion to enrich the debate but also to look at how, you know, if we talk about child pornography and some of the measures that are being proposed, what are the implications for other users.
I think I'll stop there.

>>JONATHAN CHARLES: Everton.

>>EVERTON LUCERO: Thank you.
I will not attempt to summarize such a rich debate that we had.
I think that I will only note some of the points that were raised. And to start with, I think that their they were complex in nature, they were, indeed, important. And perhaps the continuation of the debate will take the path of looking for a balance

between security, privacy, and openness, which is not an easy task given the multi-dimensional nature of the issues that no solution fits for all.
The problems that were raised today, the questions that were posed here, they represent challenges not only to law enforcement agencies, but also to parliamentarians, to civil society, to intergovernmental organizations, to the private sector, to the technical community.
So whatever the way forward may be, it has to go through the multistakeholder cooperation, dialogue and partnership in the spirit of shared responsibilities.
That is drawing the line between privacy, security, and openness is, indeed, a collective work.
We have to start somewhere. I think it is about time for us to move from this course to action, and it would facilitate that if we start in an area where there is a clear common understanding of what needs to be done.
For instance, one of the issues that has been debated at length today was the question of child protection against sexual abuse and pornography. And it seems that discussion has matured enough in this area so that now we perhaps could think of creating a common environment where all relevant stakeholders could build trust and work together.
And the IGF in these discussions certainly facilitates that and can continue facilitating it.
We need to remember the need of enabling developing countries to fully participate and share their needs, challenges and concerns, and we also need to remember that we are not starting from scratch. We are not reinventing the wheel. There are relevant references, there are international norms like the Universal Declaration of Human Rights, among others. And there are national and regional experiences that are, indeed, useful and are already there, as we have heard from many who participate in this debate.
And to finalize, my last point is about the need for a long-term solution, which is not only based on law enforcement but also on the quality of education, on educational quality, devoted to raise consciousness and awareness towards personal empowerment, fulfillment, and above all, happiness, so that we may become integral human beings that we are all meant to be.
So that's what I would like to say to finalize.
Thank you very much.

>>JONATHAN CHARLES: Everton, thank you very much.
Let me tell you, we are going to continue this debate at 11:00 tomorrow morning in a workshop in room 2 on the future of the Internet. I will be chairing that and certainly these are issues that we'll be taking on at 11:00 tomorrow morning in room 2 on the future of the Internet.
Let me also tell you about the dinner tonight. There is a cultural event, dinner which is at 7:30.
The shuttle service is going from here to the dinner venue from 6:30 onwards, so there are buses out there, and delegates are obviously invited to use that shuttle service.
The dress code is informal and there will be a shuttle service afterwards from the dinner venue back to the hotels and that will start at 9:45 going back to the hotels.
Thank you, indeed, for taking part today. Thank you to our moderators, to our co-chairman, both of them. A very interesting debate.
[Applause]