Internet Governance Forum
Hyderabad, India
Fostering Security, Privacy, and Openness
4 December 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.

>>CHENGETAI MASANGO: Hello. Let's start the next session, please. We are starting the next session which is fosters security, privacy and openness. The chairman is Mr. Shyamai Ghosh who is chairman of the data security council of India. And he is also -- was with the Indian administrative service, and his major assignments have been secretary of telecom and secretary of information technology in the government of India.
So he is very knowledgeable about these issues and I will hand it over.

>>SHYAMAI GHOSH: Thank you, and a very good morning to all the distinguished delegates.
We have a very interesting subject before us, particularly following from the previous session.
Fostering security, privacy, and openness.
I would add to that the right to information, which is a building issue in our country.
I am sure the panelists will address whether it is conflict situation or a converged situation.
Conflict in the sense of national security versus security for privacy, and the right to information. Convergence in the sense of security, privacy and openness being mutually reinforcing preconditions for users.
And by stepping up levels of user security and privacy, confidence is engendered for use of Internet and facilitates free expression of opinion.
Here, there is a very critical issue which we, in the data security council, had an annual event previous two days -- we had intentionally had it in Hyderabad -- whether there is an issue relating to culture of privacy.
Internet is global, but privacy could be local, could be regional, could be national.
And a very simple instance of this is an issue which is debated here: Whether your tax returns should be open for public view.
I know politicians have to declare their assets, but should it be applied across the board.
As is becoming clear, Internet has become a way of life, for the young and particularly old like us who are self-employed and we can't do without the laptop 24 hours a day, 7 days a week.
In this context, is Internet governance a relevant issue?
And too long in this business, 15 years ago, if you use that, Internet has been free and it should continue to be free. But there are societal issues which need to be addressed and, therefore, governance becomes a relevant point.
In the Indian context, since we are here, we have an amazing story where 9 million subscribers are being added every month.
We have gone from 2% penetration of telephones in 2000 to 30% now, but there are challenges.
The rural population is still to be covered. How can they be brought into the mainstream?
Internet broadband penetration is very, very low still. And one of the challenges which I faced as the administrator of Universal Service Fund is how to reach out. And a solution which has been found is to support infrastructure through the universal obligation fund to fund infrastructure, which will be shareable. And that will be the towers which will help

penetration in the rural areas.

Wi-max is a solution which we have eagerly looking forward, but at the same time, the incidents of the past few months had brought out the need to create user awareness for technologies like Wi-Fi. Your identify can easily be stolen, if you are not careful, you don't know the do's and don'ts in this regard.

Without taking up any more of your time and the time of my panel, I will now hand over to my esteemed colleague, Mr. Gross, whom I know for the last eight years, and he will now take over the management of the panel.

Thank you.

>>DAVID GROSS: Thank you very much, Mr. Chairman, and welcome to everyone here to what I think will be, far and away, the best panel of the entire conference.

We're going to try to do something a little bit different.

In the spirit of the IGF, which among many other things is an experiment in self-governance and Internet governance, we're going to try a slightly different approach than the first panel in a way to see if this works as well.

What we're going to do is I'm going to give a couple of remarks. Then I have asked each of our esteemed panelists to talk for about five minutes on a subject that is close to each of their hearts and their professional experience. And then we are going to try and engage in a dialogue amongst the panelists, and we will try -- I will try to make it, at least, as interactive if not controversial as possible, recognizing that people have jobs to go back to and they don't want to be too controversial.

At the end, we will try to take some comments from the floor, so be prepared for that. We will try to do that in a way that will not interfere or take away from the open dialogue of this afternoon where there will be lots of opportunity for discussion as well.

Let me begin by a couple of thoughts.

One is that the issue of security, privacy and openness is, in my view, going to be the center piece for policy discussions for the next many years.

I say that in part because if I look back on the past eight years or so, these have not been the front-burner issues. They have been issues, they have been serious and important issues, but issues that people have talked about in terms of Internet governance have really focused on many other areas and have been much of the focus of things like the World Summit on the Information Society and many meetings.

Which is an interesting situation because if you go back into the 1990s, the issues that we are going to be discussing here were, in many respects, the burning issues of the day. And what I would suggest is that those embers have continued to burn and are about to flare up because they discuss, really, the confluence of societally important issues that are, in many respects, in conflict with each other and yet are additive of each other: Security, privacy, and openness.

We have a terrific panel here that has great expertise in this area. I will note in the interest of trying to make sure that everyone takes away something that maybe is useful, I want to just sort of list a couple of the more recent relevant -- what I think are the relevant international statements that are important in this area, not in any way to be an exclusive list but just the ones that I find myself referring to with increasing frequency.

Of course, I always begin with the universal declaration of human rights with regard to the free flow of information and its importance. I think, of course, of the World Summit on the Information Society, and that was particularly in the Geneva phase, there were good statements there, but in my view, the Tunis Agenda was a high watermark for the commitment to free flow of information, both in paragraphs 4 and in 42 are the two that I often refer to.

Just this year, we have had a number of important developments that I hope panelists will refer to. One is the OECD ministerial that we had earlier this year, and there are important statements there on the free flow of information.

Just very recently, the International Telecommunications Union met in South Africa at the World

Telecommunication Standardization Assembly, not often thought of as a place where, at least, free flow of information issues are discussed. But in fact, resolution 69 that was offered there is, I think, an extraordinarily strong statement about the free flow of information in which member states were invited to refrain from taking any unilateral or discriminatory actions that could impede another member state -- and it was made clear that "member state" includes its citizens -- from accessing public Internet sites.

That means, in my mind, that countries around the world have now unanimously and by consensus agreed to allow their citizens to have access to the world's Internet sites.

And then very recently, in a nongovernmental context, there is the Global Network Initiative that a number of NGOs and companies came together to try to address the issues of protecting freedom of expression and privacy for users in ways that are , I think, very ingenious and very, very interesting to look at.

With that brief set of comments, let me begin with John Carr who is the secretary of Children's Charities' Coalition on Internet Safety in the United Kingdom for a few opening remarks.

John.

>>JOHN CARR: Thank you very much, Mr. Chairman.

And my highly truncated remarks follow.

It was interesting the treatise and documents that you just referred to as being the cornerstone of many of the debates that we're here to address.

What you didn't mention, and, in fact, what almost always, in my experience, gets omitted is, for example, the United Nations declaration on the rights of the child. The European Convention on Cybercrime.

These are just two important international documents, important international treaties which, for example, create specific legal obligations on states and actors within states to provide for the protection of children.

And what I think hitherto we have not seen addressed adequately is the way in which we integrate and balance the obligations on states, the obligations on adults in general, on businesses and so on to provide adequate protection from children and how you balance and address those with the other rights referred to in your opening remarks in relation to, example, free expression, privacy, and so on.

There are tensions. I think they are tensions which can be resolved, but nonetheless, they have not yet been fully addressed, in my opinion, and perhaps today's session will see the beginnings of a more serious discussion on that.

Very briefly, as we know, children have been and will remain major beneficiaries of the new technology. Most children have no fear of the technology, none at all, unlike their parents. And as we say in English, they have taken to it like ducks to water.

And so children and young people generally are benefiting very specifically from what the technology can deliver. But wonderful though that technology is and fantastic though the range of opportunities that it's opening up for children and young people in general, we cannot remain blind to some of the down sides of not yet being adequately addressed.

There are five broad categories of risk that we need to bear in mind when we think about children, young people's use of the Internet. Content is the first and most obvious issue. That's to say the Internet's ability to expose children and young people to age-inappropriate material. Some of it may even be illegal material; for example, such as child pornography. There are other issues in relation to contact, the way the Internet is able to facilitate exchanges, for example between sexual predators and vulnerable children. And numerically, this is by far the more important issue for children and young people, the way in which the new technology is facilitating and enabling new styles of insidious bullying and online harassment.

There are issues in the field of commerce, the way in which some Internet companies, rather unscrupulous companies in my view, seek to sell to children and young people, take advantage of their less worldly-wise ways, dodgy products or to misrepresent the terms on which those products or services are to be offered or in which they seek to obtain commercially sensitive or commercially valuable information from children; again, taking advantage of their naivete.

There is the question of addiction, the way in which some children appear to be drawn into overuse of the technology, which can be at the expense of normal and healthy development of social relationships, taking exercise and that type of thing.

And finally in the list of areas of concern that we need to think about is the issue of privacy. And that cuts across several of the ones that I just mentioned. But what right to privacy does a child have, a legal minor have vis-a-vis its parents, vis-a-vis its school. How do companies determine whether or not they have in fact obtained true consent from someone old enough to give it? And it's a very basic level. If you think of commerce on the Internet, how do companies know, for example, if they are selling an age-restricted product to somebody that is legally entitled to buy it? We have had several cases in the United Kingdom where children are buying alcohol, tobacco, knives, things of this kind and getting the companies to deliver it to their home.

They couldn't go into the shops and buy these things because the shopkeepers would see that they were children and simply prevent them from buying those goods. And if they did, they would be breaking the law. But these things are being supplied to children over the Internet. They don't even have to have the inconvenience of having to carry the goods home. The companies will deliver them to their doorstep.

And these are, it seems to me, some of the issues that we need to think about.

One plea that I want to make, and it's a very heartfelt plea. When companies speak about and when Internet companies speak about and governments even speak about reaching out to children, reaching out to families and reaching out to parents, all of which are very, very important, they seem to think that all children have got identical IQs, identical -- live in equally stable family settings and have got an equal facility to receive, understand and act upon the messages.

Parents and families are all somehow modeled on some notion or idea that, in my experience, doesn't exist, certainly doesn't exist for every child.

We have to get more sophisticated in the way that we think about approaching children, young people, and thinking about how we support families and parents to help their own children.

>>DAVID GROSS: Thank you very much, John.

Now we're going to turn it over to Jac Kee, who is a member of the Association for Progressive Communications for a few comments from her perspective.

Jac.

>>JAC SM KEE: Hi. So I'm going to introduce into the whole debate about privacy, openness, and security the dimension of women's human rights. This is particularly critical, because, historically, by introducing women's human rights into particular debates, it has not only deepened our understanding of what the issue is, but also has facilitated more inclusive and comprehensive responses.

So, in particular, I would like to speak about today is on the issue of sexual rights. Why are we talking about sexual rights? This is because in this area of content regulation, sexual rights is often brought up as a form of discourse that's mobilized to justify content regulation interventions or to talk about issues related to openness, security, and privacy.

And, in particular -- so what are sexual rights? Sexual rights is basically a state of physical, emotional, mental, and social well-being that relate to sexuality, not merely the absence of disease, dysfunction, or infirmity, but it also requires a positive and -- approach to sexuality and sexual relationships as well as the possibly of having pleasurable and safe sexual experiences, free from coercion, discrimination, and violence. And this is from the Cairo program of action.

So numerous human rights have a direct bearing on what -- on sexual rights and sexual health. This includes right to liberty and security of the person, right to be free from torture and inhuman and degrading treatment, right to private and family life, right to nondiscrimination, and, importantly, right to information and education.

So we're looking at these three sort of -- what has been raised as three concepts that apparently are in tension with each other. We are talking about openness.

The free flow of information, the ability to be able to acquire relevant and timely access to information that directly impacts upon your life.

When you look at sexual rights and women's sexual rights, in particular, this is very critical, because we are -- the Internet is not -- it doesn't exist in a vacuum outside of social relations. We have to locate this within the social, political, economic, and cultural context that we exist in.

So sexuality -- women's sexuality has often been constructed as a kind of lack, as passive. And it has a whole cultural connotation of shame. It's hard to exercise sexual agency without some kind of cost on the individual.

The Internet has provided a kind of critical space to enable women to explore and self-author their sexual agency, to be able to acquire information about sexual and reproductive health that may or may not be available in other sorts of public spaces, for example, about abortion or about negotiation of condom use by teenaged girls, and so on and so forth.

And also about exploring a more positive form of -- and a more active form of sexual expression. So the Internet has also facilitated what is now known as erotica, so sort of depictions or expressions or explorations of sexual encounters, behaviors online made by women for women that puts women as the sexual actor, not as the object that is being acted upon, which is found in most mainstream pornography.

It's also become a critical space for women of marginalized and diverse sexualities to network, to exchange information, and to be able to build communities with each other. And this is where it also intersects with issues of security -- sorry, issues of privacy. So it becomes very important for people -- for women who are accessing information online, who are interacting online to be able to feel safe in the space to not be subjected to intrusion or surveillance either by people within their community, their families, for example, for a domestic violence survivor, it's critical for her to be able to go online to find support information, and for her cache and cookies, that it's possible to delete this in her footprints online. Or for state intervention, there are communities working on diverse sexualities in very prohibitive contexts who found it very necessary to be able to learn tools on secure online communications to anonymize themselves and to build Web sites based on this, because it's critical for them to be able to mobilize and advocate for their rights.

And in terms of security, this has -- this is quite interesting, because it's also raised -- we're starting to realize the different forms of security issues there are for women who are accessing online spaces. So the intersection between violence against women and communication rights has revealed the many dimensions of power relations that exist in this online space that either amplifies or disrupts what's happening in our social spaces. So, for example, things like online harassment or cyberstalking, which we are only beginning to sort of unravel and understand its impact. We know it happens. It has happened before on the streets and now it's just happening on digital spaces.

Things like using GPS technology to track spouses who are being controlled in domestic violence situations, and at the same time, the reclaiming of these technologies to disrupt what it's being used for, so that's a very famous instance of women in Afghanistan who put video cameras underneath their burqas to be able to document immediately and directly violations against the women's rights in very oppressive situations and use the power of the Internet to be able to safely and anonymously disseminate this through a video viral.

So I suppose when you think about this, and by casting a sort of a lens that understands dangers and risks to certain kinds of rights, not just in terms of the state versus the individual or the corporation versus the individual, but also in the more shifting dynamics of social relations between individuals and individuals, whether in a family or whether in a social context, and things like, for example, privacy becomes interesting.

The concept of privacy have not been very kind to women in general when it's applied in law. So, for example, in situations of -- it took many, many years for domestic violence to be understood as a crime against the state and a public interest issue, because privacy was understood in the -- in our imagination as a domain, a space. It wasn't linked to the body. It's not a bout privacy of myself, but it's privacy of my home. And the home belongs to the head of the family, which is usually male. So then it's the intervention into the home becomes a problem because you're intruding into the right -- the man's right to privacy.

And I think I have one minute left. So maybe I will just leave it for the discussion later. But I guess I just want to end with a few sort of -- a few questions. One is, when we talk about harmful content online and we talk about harmful practices such as what's happening in social networking platforms, we must locate it in its social, cultural, political, economical context. This is relevant, it is connected very much to what's happening in the real life. And when we talk about harm, then we can't be simplistic about this harm as well. We have to interrogate it, unpack it, what is this harm, to whom? Who defines it and who participates in this decision-making?

And I will leave that for the discussion later.

>>DAVID GROSS: Thank you very much. I think that's going to highlight, for example, we're going to have some interesting by plays here.

[ Applause ]

>>DAVID GROSS: For example, the issue of women's rights, particularly with regard to sexual issues and the like, versus the issues that John highlighted, which is children's concerns, where and by whom do the lines get drawn? Who is a child? At what age is that changed? Is that a uniform global phenomenon? Is it a local issue? Is it a -- what is the role of governments? These are the issues I think we can express and have some interesting dialogue on.

And with that, Joe, Joseph Alhadeff, who is the vice president of global public policy and the chief privacy officer at Oracle, who generally on a day-to-day issue doesn't deal with those issues, but will raise some other interesting issues.

>>JOSEPH ALHADEFF: Thank you. I'm going to start by actually referencing one of the documents that the chair brought up, which was the OECD recent ministerial in Seoul and some of the issues in the declaration, just because it -- taking a step back, it gives us a little bit of context as we look at the concepts of privacy, security, and openness.

And one of the things that the ministerial came to the conclusion of was the importance of information flows, ICTs, and innovation to economic growth, to societal interaction, and to the benefits that arise, while recognizing that there are risks associated with the use of these technologies and the need to address them in an appropriate fashion.

And that was an interesting concept, because I think we have to understand the utility of this context as we look at it and as we look at the potential benefits and tensions that are inherent in the overlap of the three topics we're dealing with.

I think a number of issues that were raised at the DSCI Nascom meeting that was referenced also are important, because we focused on the cultural aspects of privacy. Privacy, unlike security, has a greater subjective aspect that is more tied to local culture. When you sit there and you look at password security, password security is not an issue of local culture. But how you deal with information and control over information has many issues that are locally relevant.

So when you start entering into a position where we have global information flows, but you still have regional and local regulation, you start understanding some of the complexities that are inherent in this space. You then take that, the concept of Web 2.0 technologies, some of these more collaborative and interactive technologies, which create the idea that information again is less tied to geography, that users are now creators and publishers and not just people who are acted upon, and that you have generational and geographic attitudes and values that are changing related to privacy.

And there you get kind of a flux and a mix. And when we take a look at those issues, we come into the area of privacy, security, and openness, and we try to figure out where's the overlap, where's the mutual reinforcement, and where's the tension.

And as we look at these, I think there was one question that was asked by one of the early speakers in the first panel that was very pertinent. And that question really was, what kind of security do you want and how much security is enough? Because those are the kinds of questions that relate to where you actually look at some of these tensions and how they're resolved. Because what you really want is, you want security to be effective. You want privacy to be respected. And you want an open framework to enable transparency and free flows of information.

And when you look at privacy and security, in many cases, you have the possibility of having mutually reinforcing concepts and technologies. I'll provide an example of -- since we are well familiar with databases, one of
the things we looked at was, when we looked at database technology, there are a lot of technologies that were built into the database initially to promote security,
so the type of audit protocols you have, the type of role-based access controls you have were very much security tools when they were built. But they have a privacy effect when you think of configuring them the correct way.

And when you think of security and privacy and you configure them to optimize the combination of both, you actually get a very interesting equation where one plus one equals three. And while that might not be good math, it's a good result.

And so that's one of the things where you have to think about how do privacy and security become mutually optimized. Because it doesn't have to be a balancing on those issues.

Now, there are going to be places where you have tensions and you do have to have some kind of balance. There is an example, for instance, of within the European Union, companies -- and in most other places -- companies have a responsibility for protecting their customer data. On the other hand, there's also a responsibility for having some privacy aspects of the workplace and respecting employees in the workplace. And there you have a tension on how much monitoring is appropriate and how you manage these issues. And that's a balancing that has to be reached.

And that's the kind of balancing where a stakeholder consultation, where consultations with data protection commissioners, are important ways of finding the appropriate resolution to those issues.

You'll find that you also have the same things with openness. So the issue of transparency, the issue of notice, they're very important issues that promote openness. You have free flows of information.

On the other hand, if you are completely open about how you configure your security, you have provided information on how to compromise your security. So that is a place where you have some tensions. If you are completely open about certain types of information, you violate obligations of confidentiality that you may have to your customer, to your employee, or to others.

So, again, those are areas where you have to resolve those tensions, but where there are also mutually reinforcing possibilities. And I guess one of the things I want to come out of this is that you don't have a simple, black and white solution of saying, it's either in balance, it's either competitive, or it's either mutually reinforcing.

It's all of those things. And the question is, how do you best optimize. You have a lot of elements that you are managing. There are ways to manage them with the greatest optimization. And one of the ways you have to look at those is, you have to have flexibility in the frameworks. One of the things that was also said this morning was a one-size solution does not ever work. In security, it doesn't work. In privacy, it doesn't work. And while the word I'm going to use has a technical meaning, I am using it in a much broader fashion than its technical meaning. What you really have to look at is how you develop interoperability. How you make different frameworks interoperate, how they work together. Because we are not going to get a unified framework of everything for everybody. And it may not be beneficial to have one. But you do have to have frameworks that talk to each other, that work together, that allow you to collaborate and work cooperatively.

And that is one of the things when you take a look at the three topics we're dealing with, really, what you're talking about is what is the effective interoperation across those three topics.

And with that, I will stop before I get a little note.

>>DAVID GROSS: You're too far down there to give you a note.

So thank you, Joe.

I think one of the issues that we'll come back on here, some of the points that Joe just raised, which would include, if one size doesn't fit all, who decides what size does fit? Is this a role for government, for self-governance, is it something that customers tell you? Is it something that you decide for yourself, how the various actors interact, particularly in a global environment?

And similarly the issues that you raise with regard to Web 2.0, social networking, and the like, obviously, has an impact on all of the discussion we have had so far, it seems to me, including the question of how much privacy is the right amount of privacy. And perhaps the changing views on the importance of privacy, as demonstrated by various people.

We're going to next turn to Professor Stefano Rodotà, who is a world-renowned, chair scientific committee of the agency for fundamental rights of the European Union. Former president of the EU group on data protection.

Professor.

>>STEFANO RODOTÀ: Thank you, Chairman.

We live at a time when the issues related to the protection of personal data feature a remarkably contradictory approach, speaking frankly, a veritable social, political and institutional kind of schizophrenia. There is increased awareness of the importance of data protection as regards not only the protection of private sphere of individuals, but their very freedom, at the same time, is internal and international security requirements and market interests are pushing towards the erosion of fundamental safeguards. The multifunctionality criterion is increasingly applied. Data collected for a given purpose are made available for different purposes. Data processed by a given entity are made available to different bodies, public and private. Reuse and interconnection are the leading criteria.

May we react to this trend and find a more sound and correct balance between data protection and security, data protection and market logic.

Look, for instance, at two important international documents, the charter of fundamental rights of European Union, and the European Convention on Human Rights. Shortly, these two texts make reference to the -- states that limitation for security purposes never can impinge on the essence of the right to data protection and they must, in any case, pass a preliminary democracy test.

Having in mind this basic criteria, and at the same time we need a positive reinvention of DP, of data protection, because the many technological and institutional changes.

For example, social networking, YouTube, Facebook, MySpace, deeply changed the context of data mining and profiling, because informations are made public by the same data subject. It means that we must rethink the rules on data collection and access on both sides, data subject and data collectors.

Second, digital person is under attack. Through massive profiling, identity is more and more built up by others. Pressures for trace-back make anonymity disappearing. Can we accept our societies be converted into nations of suspects? The transformation of people into naked individuals?

Third, we are facing changes of the same body, because the diffusion of devices like electronic bracelet, wearable computers, microchips on the skin that can be read through the technology of radio frequencies. Can we accept people be converted into networked persons, tracked and traced, configured little by little, in order to transmit signals so that can be continuously controlled. Finally, it has been proposed the retention of all data produced by people, a perspective dramatically risky in the perspective of the coming Internet of the things. Can we accept this digital tsunami?

Answering these questions, we can find a renewed and strong legitimization for data protection looked at by many people as a fundamental, fundamental rights.

Thank you.

[ Applause ]

>>DAVID GROSS: Thank you very much, Professor.

Our last presentation, formal presentation, will be given by one of the great champions of free flow of information and freedom of expression. He has worked tirelessly on those issues through many forums. We spend a lot of time together at the World Summit on the Information Society, where he was really a champion of the free flow of information. Abdul Waheed Khan is the assistant director general for communications information at UNESCO. He gave a fabulous speech yesterday.

Mr. Director General.

>>ABDUL WAHEED KHAN: Thank you, Mr. Moderator. You have given away what I was going to say.

But, anyway, coming from UNESCO, representing UNESCO at this forum, I'm sure you will not be surprised if I take you back to UNESCO's constitution that was created some 61 years ago. And that constitution talked about free flow of ideas, information, and knowledge. And you mentioned several declarations in recent times that have reiterated this fundamental principle of free flow of information and knowledge. And this, of course, is anchored in article 19 of the Universal Declaration of Human Rights, freedom of expression and freedom of the press.

But, again, in recent years, we have talked about this fundamental principle not only applying to the traditional media of printed press, radio and television, but to new and emerging technologies, what we call the freedom of expression applying to technologies without frontiers.

I'm sure when you look at the emergence of new technologies, there will be new other technologies developing, and, therefore, as far as we re concerned, the fundamental principle of freedom of expression should not be compromised, whether in respect of old medium or new medium.

If you recall, if I can take you back to the World Summit on the Information Society, UNESCO advanced the notion of building knowledge societies. And we talked about four fundamental principles of building knowledge societies: Freedom of expression -- of course, you will not be surprised that that was one of the major principles -- universal access, respect for cultural linguistic diversity, and quality education for all.

We believe that openness, the concept of openness, applies to each of these fundamental principles. Freedom of expression, it is obvious. But when you talk about universal access, how can you have universal access without relying fundamentally on the concept of openness? You -- the respect for cultural and linguistic diversity, likewise, has to rely heavily on the notion of openness. And quality education without openness in Internet, you cannot really expect this technology, what we refer to as flexible learning or e-learning or online education, et cetera, again, will be restricted without relying fundamentally on the basic principles.

And yet there are attempts made to curb freedom of expression and free flow of ideas through technical means. These are, for example, filtering or blocking software on servers. Financial means, such as high taxes and tariffs. Legislative, special laws to block, for example, sites.

So attempts are made to curb openness and freedom of expression on the Internet.

In our view, the fundamental principles that must be -- that must govern the Internet and its structure must be transparent and democratic, multistakeholder approach, of which I mentioned yesterday, and several other speakers did, facilitating access for all, and ensuring stable and secure functioning Internet.

Now, in -- Mr. Chairman, in your remarks, you mentioned that the security, privacy, and openness on one hand may appear to be somewhat conflicting ideas. But on the other hand, you can also think of convergence between the three. And I think the world will be a better place if we look for those convergences. However, in doing so, I would strongly urge that we maintain the principles of openness and freedom of expression as a priority element in any future discussion and policy-making decisions.

Thank you, Mr. Moderator.

[ Applause ]

>>DAVID GROSS: Well, thank you very much.

Now we're going to try to do the more controversial part of this program, now that we've had the opening comments. And so I'm going to try to start by asking a couple of what I hope to be reasonably provocative questions to talk about what I think are at least the tougher areas, the grayer areas of where these things come together, with the hope that then our panelists will ask each other. And the idea here is to have some interaction, which I will share with the audience is hard when we're all facing out rather than to each other. But we'll do the best we can.

And, John, I'm going to put you on the hot spot first, if I may.

Jackie made what I thought was an extraordinarily articulate set of statements about the importance of communication amongst various people to talk about issues that are, of course, of great importance to people, their human sexuality and the like. I don't think we mentioned that age was a particular issue necessarily.

You have talked about the rights of children. You have talked about content and concern about contact and the like.

Let's take off the issue of child pornography, just because that's, in my view, the easy case. I don't know anybody who is for child pornography.

Let's talk about teenagers, who are generally considered to be children, but yet have a lot of indicia, particularly in many countries, have a lot of the rights of adults. They can often marry at certain ages and so forth.

Tell me a little bit about how you, and by whom, should draw the line about issues of importance to women for teenaged women to have access to sexual information and to be able to communicate with each other.

>>JOHN CARR: Well, clearly, it's incredibly important that teenaged women, teenaged boys, for that matter, can get access to relevant and appropriate information about sexual health. If they weren't able to do that, not only would they be putting themselves at risk, but also they'd be putting other people at risk.

I don't -- I don't have a problem, in principle, with any of the points that were made by Jackie in her contribution.

The issue arises, really, in a broader context, which is simply, you know, every society that I'm aware of has passed laws and/or has quite strong social conventions around what's considered to be acceptable for legal minors. I don't see a reason why the Internet should be exempt from the same conventions and the same rules in principle. And to some degree or another, I think we're still all struggling to come to terms with some of the rather windy rhetoric of the early years of the Internet, when it was seen as completely, you know -- providing a means of, essentially, doing away with the old alder altogether. Well, now that you buy your Internet access with your TV, or in shops that -- the Internet's become, essentially, a consumer product, it's a family product, hundreds of millions of children and young people are using it, we can no longer think about the Internet and Internet policy without also thinking simultaneously about how this or that decision will impact upon hundreds of millions of young people.

And yet, I mean, you mentioned, for example, the document produced by the Global Network Initiative. There's no discussion in there about the rights of children, the rights of young people. There's no attempt to balance, in that document, the issues of how the Internet is impacting upon young people and young people's development. And I think that's very regrettable.

And I hope the same energy and resources and impetus that was behind the development of the Global Network Initiative, for example, can be put behind a debate about how we do balance out these different tensions and different conflicts.

>>DAVID GROSS: Jac Kee, let me turn to you and ask did that sound right to you? Do you believe that it should be left to traditional norms, which are often government-created norms, to determine rights of information for teenagers, non-majority children, but yet have a lot of the indicia of adults?

And you mentioned the issue, for example, in repressive societies, at least repressive for women, the issue of trying to make sure that people know about what's happening there. What is the appropriate role for governments? Is it national? Is it up to the individual? Is it up to the family? How do you view these?

>>JAC SM KEE: I think that the role of governance, and when it comments to Internet governance, really the primary function of it is to see how you can create an Internet that empowers the users and the people to be able to realize the multiplicity of their rights. And these rights are -- you know, rights are not neutral as well. They are

not apolitical.  It's not immediately understandable, as you were talking about women's and human rights.

And I think the problem -- not the problem but the difficulty that comes with when talking about protection of children is that it's -- and lso about sexually explicit content.  This is where we talk about regulation of free flow of information. This is where we talk about setting boundaries of what can and cannot be done.

And in many times, it is writ in very noble -- or not noble, but very genuine kinds of intention to protect and to create safe spaces.

But when we rely on norms and when we rely on, especially -- norms means things which are normally accepted as correct and things which are deviant from the norms are those which are punished or sanctioned.  And the Internet actually is a very, very valuable space to explore what is considered as deviant norms, especially when it comes to issues of as sexuality.

So, for example, in a country where abortion is illegal, the Internet becomes a critical space to find out more about what this means, what the processes are, who can help you and what kind of decisions you can make about your own body.

We do live in a gender disparate world.  You know, in all the institutions where decisions have been made and disseminated about norms -- whether it's mass media, whether it's the government, whether it's religious institutions -- you will find there are not many women present who are able to engage and participate in this decision-making, whether formal or informal.

>>DAVID GROSS:   Secretary Khan, let me put you on the spot here.

You spoke beautifully, as you always do, about the importance of free flow of information.

We have heard about the role of protecting children and the role of governments and other traditional norms.  We have heard articulately about the importance of access to information, particularly global, because you can get access to important information about yourself and about the changing norms and the like.

Who sets the limits?  Who sets these things?  Is this for governments?  Families? It can't be, as we have heard, one size fits all.

How do you try to analyze this?  Who are the actors and how do the decisions get made?

>>ABDUL WAHEED KHAN:   Difficult question.  When we met this morning, I said I would be happy to answer easy ones.

[ Laughter ]

>>ABDUL WAHEED KHAN:   I never promised to answer a difficult question.

Clearly, I think one of the things that we, as human beings, are empowered, really, i s to look for solutions.  No (inaudible) is forever.  And no law is forever.

However, there are certain fundamental issues, such as freedom of expression which I mentioned in Article 19, that it is the world adopted Universal Declaration of Human Rights, and that is where it is enshrined.

Now, most societies find their own -- or legislate their own laws to deal with the specific issues.  If certain activities are regarded as criminal activities, the law of the land is often able to deal with those activities specifically.

But that does not mean that you dilute the fundamental principles; in our case, the freedom of expression.

There is no need for doing that.

I think most governments are in a position to legislate laws where to deal with the specific issues.

This has been our stand always, and we see no reason to change that view.
Thank you.

>>DAVID GROSS: Joe, let me put you also on the spot here, and since you are the representative of the corporate world here, I will probably do something completely unfair because it really doesn't involve Oracle as far as I know. But we've talked a little bit here about the role of individuals and families and governments in making some of the rules with regard to free flow of information and these difficult issues, but there is also an important role, and you touched on this a little bit, with regard to companies, and particularly for ISPs and the like.

For example, just this past Sunday in the New York Times magazine section, there was a fascinating article that talked about the role that Google has played in trying to work through these issues of trying to balance various laws that are global, that affect a global company like Google, their customer service agreements that restrict the types of information, particularly sexually explicit information and the like that people can put on there, and the issues about how those decisions are made and by whom are they being made.

How do you think these issues should be dealt with? Are these issues that the free market can determine? You can determine your own ISP based on their policies? Is it left up to governments? Is it left up to individuals and to families? Or is it left up to companies?

>>JOSEPH ALHADEFF: Well, I think when you look at these issues, you have to look at the fact that there is a multiplicity of factors that you are dealing with. And what you have in the market is a number of different styles. And this issue isn't a new issue.

When you first started having service providers on the Internet, there were different models. There were some models where they were trying to create a safe place for families, and so they limited content in a much more dramatic fashion.

There were other ones that were merely giving you connectivity and they weren't really limiting access or content. And there were some who were attempting to take people who hadn't really had familiarity with the Internet and attempted to give them the guided tour. And so you had hot buttons to hit certain types of content and certain types of Web sites.

And I think what you end up having is, there is no one entity that can make all of the decisions.

Companies will take things that are appropriate to business models, appropriate to the laws they operate under, and will attempt to factor those in and provide notice of how they have done that factoring. They cannot provide kind of transparency to the level of individual decisions because you will stop being able to do any business if you get to that level of granularity.

But the framework conditions are usually something that are disclosed in the policies or terms related to the Web site.

And that, then, enables consumers and citizens to make certain choices about what type of sites they want to use and what they can expect to get from those sites.

And I think what we really have is there is no longer the bright line there used to be between -- I mean, in some industries, there stills but on the Internet, it's much more of a community-based concept now than it ever has been before. And the idea that there is just pure regulation and just pure actors upon which regulation takes place is no longer really the fact.

You have people who are engaged in working with people who are in regulatory structure. So you have public-private partnerships and ways in which those discussions are happening.

You are having much greater communication with stakeholders in the process as well.

And much more collaboration and consultation.

And I think the dynamic that we haven't yet come to which will change this even further is when users become their own publishers.  Because there, it's not a corporation anymore. It's a person on their own computer who is creating a blog or creating other things, and they might still be using an ISP for the communication, but they are, in many ways now, an actor in and of themselves and they are interacting with many others on the Internet and they are posting and creating content.

And so that will, again, change the dynamic.

So I think we are in a fluid area, and the answer is everyone is part of the team in terms of making decisions because it's a question of a multiplicity of options, a multiplicity of ways of doing things.  And I think there is a need for inherent flexibility, but you do have to get to the point where abuses that may be created because of that flexibility also need to be dealt with.  And that's where we get to, what you called, the more obvious things such as child pornography is something that has to be dealt with.

So you can't have a Web site that says we would like to promote and post child pornography. That is just not acceptable.

So there are some norms beyond which you don't go, but I think there is a large flexibility among the other things.  And choice, in many ways, actually helps people.

>>DAVID GROSS:   Professor, Joe touches on this idea that basically you let a thousand blossoms bloom here and let people pick which flowers they would like.  Does that really work in a global environment where you have various cultural, historic, and other norms that are important to people, important to cultures?  Something that's acceptable in one place is unacceptable elsewhere, and you have people having access or perhaps even being able to be required to see things as they go through the Internet, as they surf the net.

How does this get worked out?  How do you see this being dealt with?  Particularly, as you point out, with issues such as self-publishing through things like Face Book, MySpace that you pointed out, where individuals are going on and posting things that perhaps are interesting to some, perhaps not so interesting to others, and sometimes regretted down the road by those who published.

>>STEFANO RODOTÀ:   You are right, because we need kind of intercultural dialogue in this field if we look at the global dimension.

In this very moment, in my experience, we are facing multi data protection models.

You know, if you look, for instance, to the European Union, there is a progressive uniform harmonization of the rules.  And this model is now an important tool in the global dialogue.  Why?  Because if you need personal data from the European Union, you must give -- you must have this legislation giving adequate protection to the information transferred in other countries.

So other countries bargaining with Europe, having relationship with Europe, must confront themselves with this kind of model.

At the same time, at the same time, when you are looking not only with regional rules -- Europe as a region of the world where data protection has specific relevance. When you look at the new phenomena, like Face Book and so on, I think we have to look to a common resonance.  In this, the Internet Governance Forum, has an important -- is playing an important role, giving support to the idea as being called Internet bill of rights, Internet rights.  That's semantics.

This is a crucial point and important approach.  We need some common rules.  But what it means, it does not mean that we have to go through traditional avenues, negotiating a convention.

We need, as has been said, a multistakeholder and multi-level approach.

It means that, for instance, for some areas, we need rules.  In other areas, we must recognize that codes of conduct are today the only valuable approach.

So I think that we need dialogue, we need global awareness, we need this idea of Internet -- I use the wording Internet Bill of Rights, as a process, not as a negotiation of traditional convention. Top down.

We are living in a world, Internet, where the procedure is more and more bottom-up.

This is the right approach, in my mind.

>>DAVID GROSS: John, go ahead, please.

>>JOHN CARR: I just wanted to come back on the point that Joe made, saying that everyone is part of the team.

That's simply not true. It's certainly not true in the U.K.

Time after time, surveys by entirely independent academics, talking to parents, for example, about their children's use of the technology reveal that the parents, a good number, absolutely not all of them, but a good number have no idea how to grapple with some of the essentially technologically based challenges or issues that their children are having to deal with.

One of our big mobile phone companies did a survey which they are showing the evidence on a video that they did as part of the process of doing the research.

Parents who have just bought brand-new mobile telephones for their children had no idea that these phones, these devices allowed their children to connect to the Internet.

And by the way, in some cases, these were parents who had, in fact, installed filters and blocks and had all of these discussions about Internet usage of computers at home. They then buy a mobile phone device and then discover that, actually, they have also provided their child with Internet connectivity through their mobile device.

Now, what do we do about this? I mean, it seems to me that you can say, well, there's nothing we can -- actually, I think what some companies are saying is there is really nothing we can do about this. It's not our responsibility. And it's just kind of tough on the kids of those parents who haven't understood some of the issues here.

But, you know, that's it. There's nothing we can do.

I don't accept that.

I think that, companies have a responsibility, if they are selling a product that can put children at risk, to provide that product in the safest possible condition that it can be at the time of delivery.

I admit after that, it gets more complicated. But certainly at the point that the computer or mobile phone or whatever it is is sold into the domestic market -- I have nothing to say about the business market and what adults do -- but into the domestic market where there is a reasonable supposition that children or young people are going to be using the device or using the connectivity, I think it is incumbent upon the seller, the vendor, to make it as safe as it can be. At the moment, it is completely the other way around. A computer or a mobile phone can be sold into the domestic market knowing there is a very high chance that children are going to be using it, and then the companies trust to luck, they trust to luck that the parent will find out that there are issues, will act upon it once they found out, will act correctly, and will sustain that over time.

And I don't think that's a reasonable way of dealing with it.

>>ABDUL WAHEED KHAN: As technologies develop, and as more and more people use media and technology, there are studies that show that the children are spending more time with both new and old media than they are spending in school

and with parents.
So your point is well taken that it's unthinkable that the exposure that they have to the media and its content will not have some kind of impact on their psyche. Definitely, there is clear evidence that that is already happening.
I am not going to address the issue of technology and what features you need to build and how to safeguard, but I was at an e-inclusion conference in Vienna only a few days ago, but that's not the only place where people are talking about digital literacy. We at UNESCO have been talking about media literacy for quite some time, information literacy. If parents need to be educated, how best to use the technology for the growth of their children. I think, first of all, they have to acquire information literacy and media literacy.
And therefore, in the new wonderful world that we live in, the three R's that we were used to, reading, writing and arithmetic, are no longer sufficient.
It is important for a forum such as this to recognize that new literacies are as vital, if not more vital, than the three R's that we have been used to.
Thank you.

>>SHYAMAI GHOSH: I thought I would comment. I was quite -- The issue raised by Professor Stefano that cross-model data flows have a different regime as compared to data available on Internet. If every country insists that you follow my rules for cross-border data flows, then data flows will never happen, because it will be impossible to replicate a legislative regime of one country in another.
So whether or not this issue could be also tackled in the way we are dealing with Internet governance, because that also deals with information flows. And Mr. Khan has raised very valid issues, in the sense you have freedom given to you. But the catch is reasonable restrictions.
What is reasonable restriction? As again, it's varying from different country to country, different situations. Whether or not there could be some global definition of reasonable restriction anticipating the circumstances of.
We are dealing with a global situation, a situation which is global free flow. I think more conventions that can be evolved at an international forum like this would help facilitating everybody, while addressing all the concerns which we have.

>>JOSEPH ALHADEFF: While we're neither an ISP or a search engine, apparently, I'm standing in their shoes for part of this discussion.
I think there are legitimate points to be made about making sure there's information about what features are available, making sure that you have technological capacity to do some level of blocking and control, especially for technologies that children may use. But I also think there's some level of responsibility that the parents need to take. 'Cause you can't set -- you can't say that any phone that may be sold in the domestic market needs to essentially be disabled from having any connectivity. Because that's not a viable option.
So the concept has to be --
[ Applause ]

>>JOSEPH ALHADEFF: Apparently there's an ISP in the audience, or a phone manufacturer.
The concept is that there has to be some middle ground. There's a principle that's in the OECD security guideline that essentially says, each according to their role. And everybody, every actor, has a role to play.
Parents buy knives. That doesn't mean all knife makers have to make dull knives,

because knives may actually occur in the home, and children may cut themselves. You can't go to that level.

And I'm not suggesting that you were saying that we do go to that level. I'm using an exaggeration argument. But I do think there's a responsibility for all actors to play in this. And you're absolutely right, there's a disparity of information. There's no question that there's unequal information. People need to do a better job of getting that information out there.

But part of the problem is parents are buying a phone without going to the phone store and saying, "By the way, I'm buying this for my kid. Is there anything I need to know?" They may think they are buying it for themselves.

We need to get to a place where there is a better understanding.

The last point is we are in a situation which has not happened before, as far as I know, which is is that the kids are much more technologically sophisticated than the parents. And, in fact, some parents who use the technologies don't use them well enough to block the kids, because the kids know the way around them.

So this is a situation where the adoption of the technology and the knowledge of the technology by the people who are, quote, unquote, at risk is actually at a much higher level than the people who are attempting to control them and create benefit for them.

So I don't exactly know the way that education can happen in this space. I think it definitely has to be a public-private partnership, where multiple venues of education are the best way forward. But I do think we have to have the concept of responsibility across the broad range of actors.

And then perhaps one comment to something that Professor Rodotà was talking about. One of the other regional approaches to privacy has been that of APEC. And there's an interesting concept in the APEC approach which has value as we look at information flows, and that's the concept of accountability. And the concept of accountability exists in the OECD guideline. It's inherent in the E.U. directive, obviously. But it's the idea that obligation flows with information. And that helps one move across boundaries. Because one of the problems that you have in an adequacy context is you have to find another region to be adequate. And that is a time-intensive and labor-intensive process which has only happened with a handful of jurisdictions to date.

So I think one of the things we learn in the accountability concept, if you look at obligation flowing, there may be contractual methods, there may be technical methods in which the information is given similar protection to that required in its country of origin but in a way that doesn't require a change of legal framework or an identical legal framework in the location of where the information is received. So that may be one of the things that we're looking at. And it's clearly something that in the European Union is being considered as they look at binding corporate rules. Because in many cases, binding corporate rules are an accountability mechanism.

>>DAVID GROSS: Unfortunately, we're now at that stage where we have to wrap up. Just when I think things are really getting hot, which is unfortunate.

Let me just suggest for this afternoon for the open dialogue a couple of additional things that were touched on but we obviously didn't have time to start to get into, and one of which Jackie, I think, alluded to, which is the issue of privacy on the Internet, that is, being anonymous on the Internet. If you are trying to get to information that you don't want everyone else to know that you're trying to access, for whatever reason, anonymity can be very important. Obviously, on political speech, anonymity can be sometimes very important. On the other hand, in an age where we have terrorists and we have a whole host of social problems that require people to be able to find out who is speaking, whether it's protecting potential predators and so forth, or protecting children from predators and the like, the ability to be able to track people down, to know who is that on the Internet, who are you dealing with, for fraud issues and otherwise, is a very tough and interesting set of challenges.

What is the role of authentication? What is the role of privacy? What is the role of anonymity on the Internet? And how does that change? Is it -- can you limit it to particular areas? Or do you have to have, as we talked about, basically one size fitting all here?

That issue, it seems to me, becomes heightened as we talk about medical issues, which Jackie was alluding to as well. The issue of privacy as medical records and other sources of very private medical information about individuals gets placed on the Net, exchanged. The importance of that for people to have access to information and have medical professionals have access to it but yet the security issues, the privacy issues of having that potentially disclosed. Those are some of the issues that I think can be explored much further. Obviously, this is a very rich and deep area.

I want to thank all of our panelists for their participation. And I want to turn it over to our able chairman.

>>SHYAMAI GHOSH: Thank you, David.

I think several issues have been raised which can be taken up in the afternoon session. It's not an easy issue to deal with. The challenge is how do you convert the areas of conflict into areas of convergence so that both the issues are addressed in the proper perspective. And there is probably a possible view that many of these will have to be decided in a multistakeholder environment. And perhaps the IGF, under the U.N. auspices, would be a proper forum for taking up this particular issue as to how do we take forward situations of conflict into convergence.

Thank you.

[ Applause ]

>>CHENGATAI MASANGO: Thank you, Chair. And thank you to the moderator and Mr. Gross. Please, can you remember to return your headphones. They need to be recharged. And also, we'll meet back here at 3:00 for the open dialogue, for those who are interested.

Thank you.