

Note: The following is the output of the real-time captioning taken during

Fourth Meeting of the IGF, in Sharm El sheikh. 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.

SECURITY, OPENNESS AND PRIVACY
Monday, 16 November 2009
Internet Governance Forum
Sharm El Sheikh, Egypt

>>MARC ROTENBERG: Good afternoon and welcome.

It is my pleasure to welcome you to this plenary session of the give IGF on the topic security, openness and privacy.

It is also my pleasure to introduce to you the two co-chairs of this session,

Minister Jasna Matic and Dr. Sherif Hashem.

Minister Matic.

>>H.E. MS. JASNA MATIC: Ladies and gentlemen, as you know, our topic in this session is security, openness and privacy.

These topics, which have been an issue for as long as the Internet is here as

we know it, they have become much more important now, when the Internet is one

thing that billions of people interact with every day.

It is a resource that we all rely on, regardless of where we come from, where

we work, regardless of our age, and the importance of security and openness is

very much enhanced by that fact.

These issues, the security, openness and privacy, are interlinked. And the key

question here is to find the right balance between them. How to balance access

to knowledge, the freedom of expression, the intellectual property rights.

The increasingly important question of privacy is now also brought to light

much more with the new social network phenomenon.

I'm sure that our panelists who are practitioners in this area

will help us all understand better how we can all, from various angles, add to this -- to the resolution of this very complicated question, and how we can all share responsibility, as all these questions can only be improved if we all take and assume our part responsibility. The governments, the companies, the civil communities. And what is an issue that I have been focusing on in Serbia, and I would like to share with you, has especially been the issue of children's security, and various threats that are posed to them.

As children are the most vulnerable group and the most trusting group, they usually are the easy targets.

And there has been an increasing number of cases where the children are targeted.

At the same time, they, of course, are the early adopters of all the new technologies, and are, therefore, increasingly endangered.

The question of privacy is a question that especially needs to be discussed.

And it is closely linked to the new media literacy issue.

In my opinion, and in our opinion, there is a broad campaign that needs to take place across the world in order for people and all the stakeholders to understand what are the privacy issues. What is the personal data and information that you should not disclose, and what can happen to you if you do.

So I hope that after today's session, we will be able to get closer to this

balance, which will be the silver bullet to these intrinsic questions.

Thank you.

>>MARC ROTENBERG: Thank you very much.

Dr. Hashem.

>>SHERIF HASHEM: While security, openness and privacy are really, as the Minister said, interlinked and they face -- I mean, we face a lot of challenges in trying to find the right balance for our societies, in Egypt, we

have, since

the age of the Internet, we have heard from our Minister yesterday that we started building the Egyptian Information Society a little bit over 14 years ago. And since then, we have faced these challenges at various levels.

We relied a lot on partnership between government, private sector, NGOs,

education, academic institution, research and development, because the issues

are changing over time, with new technologies emerging, with new societal ways

of making use of technology. We have seen nowadays the Web 2.0, the social

networks. They have changed the way the Internet looks and what the Internet

means in terms of challenges and opportunities for our population.

And we need to set, I mean, the right environment, the right ecosystem for this

to be a healthy environment for them to do business, to interact, for education,

for cultural exchange, for various applications that we can envision that will

emerge over the Internet that will involve our societal development.

In Egypt, we have tried to involve our key stakeholders, whether from

government, private sector, academia, to set up the right strategies for

security and for openness and for privacy in drafting new cyber laws that would

help protect our society.

In setting up, and that's more on the government responsibility, a CERT, a

Computer Emergency Response Team, at the national level.

At the same time, we coordinate our efforts with the private sector, the ISPs,

the solution providers, to make sure that we have a national program for -- I

mean, availing high-level professional training on security issues in various

sectors, whether it is ICT sector, banking sector, finance, educational and

others. Because the community could be at risk if we don't have the right

human, I mean, resources and skills to be able to cope with the security issues.

We have also partnerships with the NGOs, and we have through the cyber peace

initiative that will be discussed a bit further in workshops on Wednesday. What

they did in terms of raising public awareness, training teachers, educating

parents and students about the possible risks and threats over the Internet for

the kids.

This is very instrumental.

The First Lady had supported this initiative, and we will hear from her later

on on Wednesday about what happened. Really, it had a tremendous impact in

getting high-level support for such awareness campaign and all the training

programs that went around it.

Partnership with the law enforcement and legal system is very important,

because it's not just about regulations. You have to have the right enforcement

and legal structure. I think some of the panelists will hit on so many issues

in relation to having the right legal infrastructure, the right regulations, and

being able to enforce them.

So I'd like to end my comment with, again, the emphasis on partnership.

We don't know -- The risks change over time, but basically all what we can do

is to have the right mix of partners to encourage our society to make good use

of the Internet and to be in link and within the partnership framework

synchronize effort to make use that we have -- that we are well prepared to face

the risks, and that the risks and the challenges don't really overwhelm our

society and don't make the society miss out on opportunities.

So I leave you with the partnership thoughts, and I look forward to the

reflections from the panelists.

Thank you.

>>MARC ROTENBERG: Thank you very much for your remarks.

Before I introduce the panelists, I would like to say a few words about the agenda for this panel.

We are proposing to cover a broad range of topics. These topics include

respect for privacy and identity theft, Web 2.0 and social networking, cloud computing and illegal Web content, regulatory models and the open architecture of the Internet, net neutrality, and enabling frameworks for freedom.

We have an excellent group of panelists to address these topics. They will be,

in order, Mr. Joseph Alhadeff from Oracle, Ms. Cristine Hoepers from CERT.br,

Ms. Namita Malhotra, a researcher in Bangalore, Mr. Bruce Schneier, the chief

security and technology officer with British telecom and a well-known author

you; Mr. Alexander Seger with the Council of Europe, and Mr. Frank La Rue, the

U.N. special rapporteur for freedom of expression.

Each of our panelists will speak for seven to ten minutes. We will have a

brief discussion with the panelists and turn it to you then for discussion with

our participants.

It's my pleasure now to introduce Mr. Joseph Alhadeff.

>>JOSEPH ALHADEFF: Thank you, Mark.

As we look at a number of the technologies that are listed in the topics that

we're going to cover, we really are starting to describe what is emerging as

really a new ecosystem within which we spend large parts of our lives, whether

it's the participative Web, whether it's some of the cloud computing aspects.

These are becoming more and more a part of the fabric of our lives, as are the

information flows that go across them.

I would assume right now, as we're speaking, part apart from the fact that we

are broadcasting what is being said, there are people who are putting their own

individual versions of what is being said by tweeting, by blogging, by doing any

of a number of other things.

And as we look at this new Web, which is really location independent and which is in many ways temporally independent, we don't really need to be in any

specific time sync on this Web, we have challenges as we look to figure out how

to apply regulation that is national by definition as we look to understand what

practices are going to apply to these global information flows as opposed to

specifically local ones.

As we look at the three topics that we are to address today -- privacy,

security and trust -- it has already been mentioned that one must understand how

to balance. And another way of looking at the balance is one must understand

how to optimize, because they are not necessarily tradeoffs. There are ways to

look at them as mutually beneficial and enhancing as opposed to trading them off

against each other.

I think we also have to look at them as essential components of trust. Trust

in the way people interrelate with each other, trust in the way a business

transaction or commercial transaction may take place, trust in between citizen

and government.

So these are the hallmarks of the issues we are looking at. These are some of

the challenges that they pose.

I want to take one principle out of the OECD security guidelines, because I

think people have already been talking about it in a certain way, and that

principle is the concept that part of the guideline says that in security, there

is a role for everyone to take that is appropriate to what they are doing in the

context that they are doing it. So there is perhaps a role for the user, there

is certainly a role for the provider or the vendor, there is a role for the

government in these issues.

And when you look at what is appropriate to the role, we have to look at the changing nature of the roles that we have today.

We have new types of services that are platforms and are not necessarily easily defined in the models that we look at. We have new ways in which individuals are interacting with these services. In some cases, becoming content creators, in some cases becoming publishers, in some cases becoming application developers.

And we would have to ask ourselves, is the current legal construct related to the responsibility of actors suited to those people, or is that too much of a burden for individuals in that capacity as opposed to commercial entities in that capacity. And those are challenges that we have to pose for ourselves and think of how that takes place.

When we look at concepts of how people work in the regulatory sphere and people work in terms of compliance and some of the terms that are now being used, two terms come to the fore quite often, and they are accountability and transparency. And part of the concept is to make sure that there is appropriate information to enable empowered decision-making by those people who use services, and part of it also is to ensure that in an accountability model, it may create methods of flexibility, so that you don't have overly constrained methods of which to comply, but you may have concepts of flexibility in how to comply that still has hallmarks of credibility. Hence the concept of accountability, which by its nature has implications towards the responsibility related to that behavior as well.

As we start looking at these issues, we start seeing if trust is one of the new hallmarks of the medium, then privacy, security, and open may become enablers of differentiation. And so one of the topics was privacy as a

business advantage.

And the question is capitalizing on the ability to communicate in a way related

to the credibility of your systems in terms of accountability, those become

methodologies in which advantage can be used.

Part of, I think, the learning process is the dialogue in which that discussion

takes place. Part of it is the utility of organizations, fora like the IGF,

where the value of that conversation is enriched by a multistakeholder dialogue.

And these are the kinds of issues that really benefit from an interchange of

ideas, not just a presentation of ideas in vacuums.

So the forum here presents a distinct opportunity in those senses.

And I think the last thing, when we think in terms of an ecosystem concept and

we think of the overarching nature of trust as a concept, we have to start

thinking of holistic approaches to this. Because you can't just differentiate

and slide apart, because privacy is related to security. The ability of people

to understand privacy and security, the transparency related to that,

accountability, are all related concepts.

So we have to consider how to take a holistic approach, which again starts to

be a multi-party, multidisciplinary and multistakeholder approach to these

issues.

As we look at designing these concepts, whether it's privacy by design, whether

it's security by design, we are looking at what is really a collaborative

process, one in which you take into account both needs of consumers and

viewpoints of consumers or users, as well as the various disciplines within

business, as well as the cultural and regulatory context within which you

operate.

And those are the solutions, these collaborative developments are the solutions

that are the more future-oriented ones which we are starting to

understand how

to put into place today.

And with that, I will turn it back to Marc and to the next speaker.

>>MARC ROTENBERG: Thank you very much, Joe.

Our next speaker is Ms. Cristine Hoepers with CERT.br.

>>CRISTINE HOEPERS: Good afternoon. Okay. I am Cristine. I work with

CERT.br. CERT.br is the Brazilian national CERT. We do instant response in our

daily lives. I have been working at CERT.br for ten years now, and daily I am

dealing with people that have been breaches and compromises and that have encountered problems.

And one of the things that are common with those people in the past five to

seven years is that the (inaudible) really are criminals.

So before we talk about privacy measures, we need to know who we want to

protect general public from. So this is one of the problems.

And the thing is that what we see today is that as more information goes

online, we have Web 2.0, we have social networks, as was pointed here today. We

have people putting information out on the Internet, and not exactly aware of

what that means, and not aware that the information goes to everywhere and that

the whole Internet can access that information.

So sometimes we debate a lot about privacy, but one of the major issues today

is actually how to make people to understand the risks is not easy. The

technology is complex, so people from technology area are not actually making

things easier, because everything is complex, it's difficult to remain secure.

And one of the problems as we see, what are the criminals are exploiting is a

lot of naive people. They are trusting. They trust what people tell them. But

that is true for as long as mankind is here.

So the thing is that technology makes that easier.

But the criminals, on top of that, are exploiting software weaknesses. So when

Joe was talking about security by design and privacy by design, I think that is the key issue. And most of the time, we see people talking about companies needing to take the lead. But I think there is more people that need actually to make policies. And every year, and more and more cases I work with, I see that actually the design of the software is a problem. But the underlying problem to that is that we don't have universities preparing professionals that know what it means, that know security implications. So we don't actually have people understanding what the problem is. And it's not only to educate end users. We need to educate our next generation of professionals. So today, everybody is actually -- I think it's true that it's very expensive to make secure software. But the thing is, why is it expensive? Because people need to learn that from scratch. No one is actually teaching that. No one is actually preparing the engineers to make a project secured by design. So today it's very expensive because the companies need to come up with that solution. And universities I think are not getting up to speed. But another thing that he was saying, we see a lot of things today about compliance and about regulations. And one of the things that I think is really a problem, and I think this is why a lot of people confuse that if I have security, I don't have privacy, is that people don't know exactly what to do to get more secure in the networks, to be more secure, so they take wrong countermeasures, and sometimes they take countermeasures that were not needed. And what we see is that actually hinders ability to implement really good countermeasures, because then people say, "We cannot implement anything."

So I think one of -- When I talk about education, it's really for us to come up

together and to understand that when we talk about security, I am, as a security professional, talk about privacy. I am very paranoid about my own privacy.

And when we talk with people that ask for advice, we always say that you need to consider privacy issues. Are you sure that you want to collect all that data? Are you sure that you need to do that? Are you sure that you need to implement this or that countermeasure.

So I think people are doing a lot of things out of compliance but not necessarily are they getting more secure. But actually as the situation is escalating they need to get in some measure.

But I don't think that this will change quickly. This is why it's really a policy issue for us to think about on how many years we would like to start seeing things change.

I that work on the Computer Emergency Response Team, we are doing the front line today to keep up with the threats. But we need to have more people

thinking about what we are going to do for the next 10 or 20 years. How are we going to prepare our next generation of professionals to think about security when they are coming up with technology, and to better understand that privacy is important, that you don't necessarily need to compromise privacy to be more secure.

So this is, I think, my main message.

I work with incidents every day. I helped develop a lot of end-user educating materials in Brazil. And we are trying to get the word to them that they also need to be part, but not only in understanding how to install a security tool, but also to understand that they need to know where they are putting their information and why sometimes it is safe or not.

So for my opening points, that would be it.

Thank you.

>>MARC ROTENBERG: Thank you very much for your comments. Ms. Namita Malhotra.

>>NAMITA MALHOTRA: Hi. I think I would like to be remembered here as the lady who came with the skull.

So basically, last year in Hyderabad at the IGF then, I remember posing a question to a very similar panel, and it is kind of remarkable that I am here today on this panel, from a cantankerous objector from the floor, to have made it here, and I think that's something to be said about IGF and the multiple stakeholder thing that a lot of us criticize might be somehow kind of responsible for why I am here today.

But I also feel that as important as it is that business and economic concerns are raised at IGF, we need to be cautioned about solely thinking in that mode.

Otherwise, incidents such as yesterday when a session was disrupted because of the mention of China's great firewall or the struggle of Tibetans will become the norm rather than the exception in IGF, and that would be a shame in some ways.

What I want to do today is to engage with notions of privacy, openness, security, but from a feminist perspective and a perspective that takes on issues around sexuality as well.

I would be looking, rather than at the whole array of all the issues that might

come up when we talk about privacy, openness, security, specifically more at

privacy, social networking, and Web 2.0, I guess, and also -- but what I would

like -- what I would think is that a number of things that I would say would be relevant to issues around openness and security as well.

To basically speak about privacy is -- and how we understand it is that it

provides in some -- or it protects a safe haven where people are able to control

the terms under which they lead their lives. It is, broadly

speaking, about

personal autonomy, the desire to be avoid being manipulated and dominated wholly by others.

This, again, has to be -- autonomy in itself has to be understood in the

context of community, culture, economic factors, et cetera.

To begin with, the feminists have always had a problem with the idea of the

distinction between private and public, and rightly so, because the notion of

private has been part of the systematic oppression of women across the globe.

And it is in private spaces that most -- that those who are -- that many people

who are marginalized are also exploited. Whether it's women who are wives,

children who are abused, domestic workers who are exploited as labor in homes.

That it is the private domain that becomes the unregulated zone of life, whether

the reproductive, the domestic, the relational and familial dimensions of

people, especially women's life, and is excluded from mainstream political and

legal debate.

And that might be a problem, and that would be a caution that from a feminist

perspective should be put up that could the notion of privacy could actually be

of use when we talk about certain issues. Are there more useful concepts such

as maybe consent.

And this is something I would like to flag off, and unfortunately I don't think

I've thought about this enough to say that I have solutions on this idea.

To put, as shall we say, the cart before the horse, I want to put my conclusion

right up, and I would like -- and that would be that in our current context, and

especially from where I come from, the Indian context, and broadly speaking from

an Asian context of a gendered world, of a heterosexual patriarchal world, it is

often the body that can lead the same life publicly that is

entitled to privacy;

that legal and social regimes that often ensure privacy of those -- ensures

privacy of those who could very well lead the same lives publicly, thus the

grant of privacy rights is also an account of privilege and hierarchy.

Before I go, I would also like to kind of run through a few examples of what I

mean when I say "the Asian context" and why I feel it's important to put that on

board, and especially in -- where a lot of people here are from the global knot

and a lot of corporate entities are located in the global knot.

It is important to talk about the Asian context and what's different and what

is so complex about it. There are instances in the last two years where an IP

address wrongly provided by an ISP has led to the arrest and imprisonment of a

person for one of -- of one person for several months. Also, several arrests

have taken place of people who have posted on popular social networking sites

such as Orkut and Facebook and it's also true that these sites such as Orkut and

Facebook are becoming sites of surveillance for state, but also for local

authorities, for local police as well.

Issues of sexuality are also important, as two gay parties have been busted in

-- or, rather, have been broken up, and in one instance the police was using the

Internet to entrap four men into turning up at a public space. So until the

moment of when the men turned -- when the four men turned up at the public

space, both the policemen and the gay men on the Web site were doing pretty much

the same thing. They were talking about fantasies, they were talking about

desires.

There are also things -- another example is that of Web boards in Thailand

where a lot of political commentary takes place but the situation of -- a lot of

political commentary takes place that is watched, and a lot of surveillance happens there for people who have made comments, again, speaking against the king, which has now translated now into a climate of self-censorship which is ensuring that people don't really speak up either in mainstream media or in alternative spaces.

The other aspect of privacy in the Asian context is while privacy measures might be being built into the hardware of technology itself in the west -- and that's a great concern for -- as well -- but at the other hand, there are ways in which privacy is implemented in the Asian context, including how cybercafés are regulated because cybercafés are the space through which a lot of people access the Internet, and they themselves are regulated.

They have to hand over identities, they have to retain data, but they also have to spatially ensure that every computer in the space is facing outwards.

So as -- it seems like a small thing, but as an example, it shows how the state really does not have much regard for individual privacy.

Another example that I would like to talk about would be in the case of

Indonesia which speaks directly to the issue of gender, where a large amount of online pornography which is provided either through phone cameras or through hidden cameras is put up voluntarily and in limited -- is put up voluntarily or without consent.

But to address this issue, the antipornography law was put forward in 2008, and

it was passed in 2008, but unfortunately the law actually doesn't address any issues of privacy. Instead, the law talks about how women should be attired

appropriately in public. It criminalizes movements and gestures that are obscene or provocative, thus criminalizing many traditional dances, many

communities in different parts of Indonesia, it criminalizes homosexuality in a country where it wasn't an offense before. The broad category of sexual material -- visual, written, auditory, verbal, movements made by humans that arouse sexual desire and offends moral values -- this is the phrase that is there in the law which is entirely subjective and vague.

And the law that is -- could have been used for protecting women against violence online or violations of their privacy is, instead, being used to limit their participation in the public sphere.

A similar example could be taken from Malaysia where the leaking of intimate pictures of a politician was done deliberately as political maneuver to denounce a respected woman politician and to try to force her off the public arena.

Therefore, it is odd that a law that is supposed to or could be used for protect women's privacy is actually ensuring that women are -- that their participation in public space is limited.

So moving on from these examples to broadly say what is it that information technology has done and what is the problem that it is posing, it can be summed up in three points.

There's virtually no limit to the amount of information that can be recorded.

There is virtually no limit to the scope of analysis that can be done. And that this information may be stored virtually forever.

And if you want to feel paranoid right now, you're free to feel so.

There -- it's also possibly said quite often that privacy means different things in Asian context, and that it is maybe not a universal idea, whereas at this point, the question to be asked is: What could be a universal idea?

In a world in which we have so many languages, it is probably hard to find some conceptual term on which even the people in this room could agree

as having a

specific meaning.

It is also true that privacy, as such, has changed in its meaning.

It used to mean, for the Romans, "private" meant that something has been taken

away and that, in fact, it was seen as a deprivation or a lack, whereas in the

modern world, the private sphere is usually enriched in the age of modern

individualism, and that basically the idea of family, of home, of leisure time,

and all these various things that we take -- that are part of what we call the

private are very much a product of this particular time that we live in, and

it's not true of, say, many years ago. And obviously, then, it may not be true

across different cultures.

Yet at the same time, that cannot be an excuse for how corporations deal with

issues of privacy. It cannot be a way in which they can say that awareness has

to be raised by the citizens themselves or by groups themselves and not by

people -- and not by the corporations, or that they have no responsibility with

regard to privacy, because it is even more important that corporations have a

greater liability in a society that is grappling with globalization, rapid

changes in technology, modernity, and modern individualism that is kind of

different from what was the context in these countries before.

I would like to also talk about the peculiar idea of privacy in public. A lot

of us put a lot of our own information out there, but also, this is in some ways

an idea that you want to be private -- that you want certain aspects of your

privacy protected while you're in public -- while you're in the public sphere or

while you're in public spaces.

In a strange way, that actually borrows the problem faced by homosexuals for

the longest time: That your most private intimate acts had to be hidden from

public scrutiny, but also had to take place in public spaces. Especially sexual activities. So homosexuals of this world are probably better equipped to deal with issues around privacy and community than any others till now. But the Internet also twists the idea of privacy in public even further and makes it an interesting dilemma for various reasons.

In the digital age, what is possible is data aggregation. Okay. Sorry.

I will have to rush -- okay. I'm going to skip a lot, and I'm going to return to my last point which I wanted to make, which is that -- which is that privacy is an account of privilege and hierarchy and that a body that does not fall within the narrow definition of normal is probably not a guarded privacy, whether it is because of divorce, abortion, homosexuality, promiscuity, or even being a victim of rape. A body that does not belong to the global knot may not be entitled to the same level of privacy because corporation entities do not recognize the rights to the same level.

A body that is female is not entitled to the same level of privacy.

A body that is not healthy is not entitled to the same level of privacy.

Definitely not a body with AIDS or even, in this age, a body with swine flu.

And these paradoxically are the bodies that have the greatest need to be able

to control how and when information is made available to others.

Thank you. I would like to end with this quote, which is "Privacy is turned

from exclusion based on self-regard into regard for another's fragile,

mysterious autonomy." Thank you.

[Applause]

>>INTERPRETER: From the interpreters, please, could the speakers speak slower.

This last speaker was too fast.

>>MARC ROTENBERG: Our next speaker is Mr. Bruce Schneier.

>>BRUCE SCHNEIER: Yeah, thank you. So I want to make several points about

privacy and data and the Internet.

The first is that we have to realize that we as a society are producing much more data than ever before, and that's not because of any malice or any design.

It's simply because computer mediated processes produce data. That's what they

do. So as the phone system becomes computerized, more data is produced. As

point of sale systems become computerized, more data is produced. As the

registration system for this conference becomes computerized, more data is produced.

So data -- every time we go on the Web, whether we're using a social networking

site or engaging in a -- in a purchase or simply surfing, data is produced.

E-mail takes the place of voice conversations. It's more data.

And this -- this data has value. And we're living in a world where a lot of

that data isn't owned by us. It's owned by phone companies or credit card

companies or companies or mediators. Social networking sites. In cloud

computing, more of our data will be given to somebody else for safekeeping.

So a lot of this data that's about us, either as persons or businesses, is not

under our direct control. And what can be done with that data is now less a

function of -- of what we want and more a function of local laws or agreements

or terms of service. And what's also happening is that data storage is becoming

cheaper. It's becoming free.

Data processing is becoming cheaper. It's becoming free.

And so as these two things drop to free, it becomes cheaper to store data of

even marginal value than it is to throw it away.

Data analysis becomes so cheap that data mining for marketing purposes becomes

a reasonable thing to do.

So we have to think of ourselves as having a data shadow. And leaving data

about ourselves everywhere we go, with everything we do. Because

more and more

of what we do is computer mediated, either online or offline. So that's the

first point.

The second trend I think is important is that I.T. is becoming a commodity.

Right?

Users are now very sophisticated about the Internet and about computers.

They're not technically sophisticated. They're socially sophisticated.

Right?

They don't know how things work but they know what should work. They care less

about details and more about results. Right?

I.T. is becoming infrastructure. We're seeing more and more sophisticated

service offerings, rather than technical product offerings, more and more

packaged solutions, so whether it's gmail or Facebook or something else, you

know, these are just all ways people can interact with computers at a much

higher social level.

I mean, moreover, I.T. is becoming a utility. Right? It's something you need.

You come to work, you expect a desk and a stapler and a phone and a computer.

Right?

It's something that has to work. And all utilities, all infrastructure is

outsourced. I mean, and this is pushing the trend towards cloud computing and

outsourced services, right? This idea that these things are becoming cheaper

and they're becoming more of a commodity.

Now, it was said before in this panel, but in this world, something that is

very important is trust. I mean, we can no longer directly affect the security,

the privacy, the reliability of our data. We have to trust our providers.

And whether you achieve that trust through audits, through contracts, through

government regulation, I mean, one way or another we as consumers -- again,

either personal or business -- need to get that trust. Because without that trust, none of this will function.

There's some talk about sort of security versus privacy, and how you balance that. I think that's a very false dichotomy. I was, you know, pleased to hear the previous panelist say that you can get both. Right? It's not security

versus privacy, is not the way to think. When you think of things like a door

lock or a tall fence -- right? -- I mean these are security measures that don't

affect privacy at all. They're not anti-privacy. The real dichotomy here is

liberty versus control. That there are -- there are things we can do to foster

liberty and there are things we can do to foster control.

And privacy can cut either way, because open government is a way towards

greater liberty. But conversely, you know, citizens with privacy is also a way

to greater liberty.

And I think that's the way to think.

And one thing that's important with these things, when you think about security

or privacy or liberty or sort of any of these important values, they tend not to

be salient. And what I mean by that is people don't think about them unless

they're brought front and center by some event, or by losing them.

These are -- when people make normal buying decisions, they tend not to think

about privacy. Only when privacy is forced in front of them do they think about

it, right?

It's not a normally -- normally a salient thing they think about. Doesn't

matter they don't care it. Just means it's not salient. And markets tend not

to be very good at dealing with non-salient features, right?

Markets are really

good at things like price, because price is always salient, or color or how --

you know, the size of the thing you're buying, right? These things are very

salient.

Privacy, security, liberty, these aren't salient. And usually whenever you have these sort of non-salient features, the way you get them in society is through legislation. The government comes and sets things like building codes.

I mean, none of us think the roof in this building is going to fall on us. We

actually don't even think about it, right? It's not salient. But the building

is strong because of -- of local building codes. I mean, and that's true all

over the world. So I mean, I liked hearing on the panel that we need notions of

accountability, of transparency. I mean, these are things we can legislate that

allow people to make smart decisions.

You know, we need to enshrine privacy as a fundamental human right, right? Not

something to be bartered away but like other non-salient things that are

important to us, it becomes legislated so there's -- there's a minimum, there's

a floor.

And I mean, I have many more things to say but I'll save that for the

discussion. Thank you.

[Applause]

>>MARC ROTENBERG: Thank you, Bruce. Mr. Seger?

>>ALEXANDER SEGER: Thank you. Alexander Seger, actually, but never mind.

For me, the key question that we have to ask ourselves -- and it's a bit along

the lines of what other speakers have said -- is how can we ensure security

while maintaining due process, freedom of expression, and privacy, and all of

this in a global environment where every country has, in a way, different rules.

I would like to underline one point here. Namely, that, yes, data protection,

privacy, freedom of expression are fundamental rights, but security itself is

also a fundamental right. I think we have to underline that. And we also have

to be clear that cybercrime and threats to cybersecurity are real threats. We

talk about offenses against computer and data systems, offenses through computer

data and systems or simply evidence on computer systems, evidence for crime. We

talk about crime for profit. We talk about organizing for crime or organized

crime. We talk about identity-related crime or the terrorist use of ICTs, and

so forth.

How do we deal with cybercrime and threats to cybersecurity and of course there

are many elements to that. There is the preventive side of this that is

extremely important. There is the protection or defensive side that is

important. And there is also, as the last resort, law enforcement and criminal

justice.

And on the criminal justice and law enforcement side, there are many things,

again, that we need to do. We need to have efficient national

cooperation, we need to carry out financial investigations to trace criminal

money on the Internet, and many other measures, but most importantly, all of

this needs to be based on law.

Law that establishes due process and that establishes procedural safeguards.

What we also should perhaps emphasize with regard to how to cope with

cybercrime is that this is a shared responsibility. In many other types of

crime, we talk about law enforcement and criminal justice institutions have the

primary responsibility. I think with regard to cybercrime, we have a role of

other public sector institutions and we also have a role of the private sector.

And we need to discuss what role can CERTs play in measures against cybercrime.

The financial sector, information security officers and companies, and so on,

and how can we all -- and how can governments, through technical

assistance --

strengthen capacities in different countries to cope with
cybercrime.

And all of this should be based on a body of common regulations,
agreements,
codes, whatever you want to call it.

With regard to cybercrime, we have the Budapest convention on
cybercrime that

is an important standard here. We have to deal with if we talk
about

counterfeiting medicines on the Internet, for example. We are also
developing

at the Council of Europe an instrument which could potentially
become a global
standard, et cetera.

With regard to data protection and privacy, we do not have global
standards

right now. There was a very interesting meeting a few weeks ago of
data

protection commissioners in Madrid, and I think there is a
potential to come to

develop some global standards and move towards global standards on
data

protection and privacy.

And data protection and privacy, yes, we need it for several
reasons.

Data protection and privacy a fundamental right. It's very
important. We have

to underline that. And we don't have to justify why we want to
have our privacy

protected. We have it as a right, and others who want to violate
it, they have

to justify why they do that.

But data protection and privacy is also a condition for law
enforcement. It is

very difficult if not impossible, and it is good like that, that
European law

enforcement agencies exchange data with third countries if third
countries don't

have data protection standards in place.

And for each of them in particular, I discussed it with Sherif
earlier on,

countries that offer off-shoring services, they also need to be
sure that data

protection and privacy standards are in place; otherwise, many
countries will

have difficulty to agree to have services and private data handled in other countries, or for a country like Egypt where off-shoring is a key business, this would be very important to develop appropriate data protection standards.

And of course, data protection and privacy helps ensure the fundamental right of confidentiality, integrity and availability of computer data and systems.

With regard to freedom of expression, due process, procedural safeguards, and other fundamental rights, it is very important to recall that the World Summit on the Information Society agreed to these values. That we have to develop capacities, we have to work towards Internet governance in full support of fundamental rights.

In Europe, we have the case law of the European Court of Human Rights which is very important, in the convention on cybercrime we have Article 15, very important, on procedural safeguards. We have, as Council of Europe, developed guidelines on how law enforcement and ISP can cooperate with each other in free respect of human rights.

I think as a reaction of the problems that some countries faced in the Far East, the initiatives were created like the Global Network Initiative that adopted principles on freedom of expression and privacy, et cetera.

So I think there is a good ground to work towards globally agreed upon and common standards, regulations or codes that allow all of us to cooperate.

And with that I want to come back to the point that Joe made, that Bruce made, that it is not a question of tradeoffs, necessarily. It is not about security versus fundamental rights. The two things have to go together. We have to talk about security and fundamental rights.

And the final message I want to bring across, we need to be able to build

capacities globally to work towards both security and fundamental rights. We

have a common agenda for all of this.

We need to support implementation of existing treaties worldwide, and perhaps

we should not just talk about creating opportunities for all. I think we should

also underline the need of exploiting existing opportunities by all.

Thank you.

[Applause]

>>MARC ROTENBERG: Thank you for your remarks.

Now Mr. Frank La Rue.

>>FRANK LA RUE: Thank you very much. Thank you for inviting me to this

panel.

I would like to begin with the last statements of my predecessor and some other

panelists, that security, openness and privacy are not in conflict with each

other, are not a tradeoff to each other. Are specifically complementary to each

other. And we have to see them as enhancing each other.

But I would also like to compliment the fact that they have to be seen from the

perspective of human rights policies and human rights principles.

In this sense, they are also to be seen as the responsibility of the user, the

responsibility of the corporations, the responsibility of those that develop

communication technology, but also and specifically the responsibility of the

state as the final guarantor of human rights exercise.

And in that sense I would like to begin with the question of openness which

encompasses freedom of expression.

These rights, specifically freedom of expression, is an individual right but it

is also a collective right. The same as communication is.

It is also the right of peoples to express not only ideas but to express their

cultures, their traditions, their language and to reproduce those cultures and

languages and traditions without any limitation or censorship.

But at the same time, I think it is crucial to see this as a right in both

directions. It is the freedom of information, or as we call access to

information, and it is on the other side the freedom of expression.

And in that sense, the question of information is crucial. It has been

mentioned. First of all, access to information of public issues is transparency. All public acts, all public activities, all public policies,

documents or information, should be put to the service of the public.

It is our documents. It is in behalf of the general interest that public

officials act and, therefore, should be to the general public that they express

this openness and this transparency.

But the same way there's different sectors. Access to information for women is

important for them to make informed decisions and their own opinion.

Access of information is important as a form of education and development of

technology and should not be limited for the technological development of a country.

There should be sort of a mentality of absolute openness in the question of

access to information, as there is in the openness to all the media and all the

forms of communication from the Internet, to the mass media, for public

expression, to the artistic or cultural expressions of all peoples.

And in that sense, we should try to remember which are the principles that we

should have applied as we exercise these human rights.

Number one I think is the principle of equity and justice. Communication

technology, communication instruments, communication facilities should not be

the privilege of few or the knowledgeable or those that can afford it. Should

be made accessible to all, as an exercise of a right by all peoples under a

nation. And in that sense, the equitable distribution of the possibilities of

communication is important.

In that sense, the net is a contribution to that equality, because

we have all
equal access. But it is also important that states do not generate
different
limitations or obstacles to that free access to information or free
access to
expression.

The second principle is the question of plurality and diversity.
There should
be the possibility of accessing different opinions, a variety of
opinions, a
variety of points of view, and not the consolidation of one point
of view, of
monopolies in communication or of monopolies in that technology.
The openness
means diversity as well, means pluralism for all that want to
exercise this
right.

And finally in the question of limitations, I do believe that the
state should
regulate. Before, it was understood that this openness or freedom
of expression
or the exercise of right meant a passive responsibility of the
state. It was
not to intervene, not to censor, and in a way, not to regulate or
to deregulate.

I think it's exactly the opposite.

The state has the responsibility to regulate these efforts to make
effective
the exercise of human rights. But we should not understand
regulation as
limitation in the sense of limiting human rights, but, on the
contrary, it is
the limitations that will guarantee equal exercise of human rights.

The only limitations acceptable in terms of freedom of expression
or access to
information are those that protect other human rights, that protect
a higher
interest or a higher value than the one they are limiting. And
those should be
very few and very qualified.

It has been mentioned in the panel today the protection of
children, for
instance. I have worked personally on children's rights and youth
rights. And
of course we want the protection of children. Of course we would
like a world

campaign and it is important to abolish child pornography, which is the not only an act of violence against children but is also incitement to violence against all children. But normally also those accompanied by child pornography and trafficking of children. So, yes, there should be specific limitations of the state in that sense.

But that should never be used -- and here is where we come to the risk.

Whether it be the protection of children, whether it be the protection of national security, or whether it be combating terrorism or combating organized crime, all of which are legitimate acts of the state and in protection of all our other rights, but they should never be used as an excuse to create a mechanism and, in this sense, the technology of filtering or of censorship, and specifically in electronic communication.

This is the big risk and which we should never allow our states or our

governments:

[Applause]

>>FRANK LA RUE: It is today, which I find and demanded in my obligation and

the reporting, that countries can use different excuses. Children is one,

anti-terrorism is another, or even the protection of religions in the world is

another. And that becomes a veiled form of censorship, because we should not

apply those criterias to limit the communication. We should apply limitations

to the effective exercise of rights by individuals, by persons, and not by

protecting ideologies, philosophies, political positions of the state or even

religions of a state. And I think this is crucial for the future of the world

today.

I also believe that we should not allow freedom of expression as Articles 19

and 20 say, to permit hate language or incitement to hatred or to

discrimination

or to violence on the basis of racial differences, religious differences or

linguistic differences, or gender or age or disability or any other difference.

But important to limit this is to be very careful and not to fall into the trap

of opening the censorship for all.

And finally, since I was invited here by UNESCO, let me say that UNESCO used to

have a program which I liked a lot which is more important to affirm the

positive in terms -- than the limitations. It was a program of culture of

peace. The alternative for the world at this moment, precisely to eliminate and

abolish child pornography or offenses or discrimination on the basis of racial

differences, religious differences or language, is to re-establish a culture of

peace as one of our new cultures in the world based on dialogue, mutual respect,

solidarity and understanding. And for that culture of peace, you have to

enhance communication, enhance understanding, and enhance freedom of speech.

Thank you.

[Applause]

>>MARC ROTENBERG: We have had many excellent presentations. If I may just

briefly summarize.

Minister Matic began by talking about the vulnerabilities of children and urged

a broad campaign on privacy.

Dr. Hashem described the importance of a partnership, particularly the Egyptian

experience.

Mr. Alhadeff described a new ecosystem and the importance of accountability,

transparency and a holistic approach. Ms. Hoepers said there are genuine

problems with criminals who do exploit naive people, but she said it was not

enough to educate users. We must also educate professionals.

Ms. Malhotra gave an important perspective on privacy and said while it is key

to personal autonomy, we must be careful it doesn't become a way of simply protecting privilege and hierarchy.

Mr. Bruce Schneier talked about the relationship between privacy and security

and said that perhaps the real tradeoff that we need to focus on concerns

liberty versus control.

And Mr. Seger urged us to focus on solutions that are based in law. And

finally, Mr. La Rue spoke to the importance of the equitable distribution of

access, the importance of accessing different points of view, and urged at the

end I think this very optimistic thought that we should engage in a new culture

of peace.

Before we turn to questions from the audience, I would like to put one question

to the panel, understanding that we have had a conversation today on the

importance of privacy, security, and openness.

I would like to ask each one of you to say what you see as the single greatest

challenge facing the future of the Internet today.

And I would ask you to be somewhat specific in your answer.

I appreciate that it might be tempting to say, "We need to find a way to

balance these competing interests," or "to promote these competing interests."

But I think particularly here, for people at the Internet Governance Forum who

are engaged in policy-making and thinking about the future of the Internet, it

would be most helpful if you could help us direct a bit the policy work in this

area by helping us to understand what you see to be the single greatest

challenge.

So I will begin with our analysts and then end with our co-chairs, if that is

okay.

Joe, would you like to go first?

>>JOSEPH ALHADEFF: I think of the challenge in much the same way of what I

described as the hallmark and that really is the concept of trust.

And how to

establish it, and what's the language that you use in these new media in order

to enable it.

And I think it's a paradigm that we are looking at, and we are trying to figure

out what is the first step, how do you make those first steps.

I think that's one of the roles that the IGF helps to play, because I think in

many cases, groups are talking at each other, past each other, or even not with

each other.

And one of the best ways to start the dialogue is to start to understand the

concerns of those people who are on the other side of you, who might be your

users, who might be your regulators, and to actually have that dialogue going.

Because without establishing that trust and that dialogue, we won't get to the

mechanisms that will be the way that you optimize rather than balance against.

So I guess, you know, the first steps are sometimes the hardest to find, and I

think that we are feeling our way at the moment.

>>MARC ROTENBERG: That's great. Thank you.

Ms. Hoepers.

>>CRISTINE HOEPERS: I would like to comment more on the challenge for the

Internet, not exactly to the IGF. But I think the challenge for the next years

that is already a challenge today is to separate what is a valid security

countermeasure from what is trying to pose as a security countermeasure just to

restrict something or to collect data.

And I think it will be very difficult for governments to deploy a lot of

technologies that are supposed to be -- to make their citizens more secure.

And they have that intention, but they are not considering what are the side

effects, let's say, or how that would affect privacy of the citizens. Trying to

do something to make them more secure, they can make things even worse.

So I think that challenge will be to separate well the countermeasures in what to do and what will actually make us more secure or not in the future.

>>MARC ROTENBERG: Thank you.

Ms. Malhotra.

>>NAMITA MALHOTRA: The challenge for the Internet, and I guess for the IGF to talk about, would be the role that powerful corporate entities have started to play in terms of data aggregation and what they can do to the data and how they use it or sell it.

And what might be interesting in that regard would be to think about privacy as maybe layered in some ways, to think about the contextual integrity of information. There is information that you give to your doctor which you may or may not want your employer to know.

So basically that I give information to some corporate entity and that it is protected within that domain.

So basically about contextual integrity, about data aggregation, and the role of powerful corporate entities.

>>MARC ROTENBERG: Thank you. Bruce.

>>BRUCE SCHNEIER: So when Marc first posed that I wrote down corporate interests, and I crossed it out even before Namita talked about that. And I thought in that some cases it's government interests.

But really the generalization here, I think the biggest challenge we face

balancing the interests of the powerful with everybody else. That it is too

easy in information technology on the Internet because of the fundamental

leverage that technology gives you for the powerful to get more powerful. And

depending on what country we are in or what the government is like, that's

either the government or it's corporations doing things that are not in

society's best interests because it's in their best interest.

And I think the biggest challenge we face is recognizing that

leverage, and
giving that leverage not to the powerful, not to the concentrated,
but the
diffuse, to the people.

And I think that's going to become a bigger challenge.

>>MARC ROTENBERG: Thank you.

Mr. Seger.

>>ALEXANDER SEGER: I think the arguments flow very nicely. And
before I saw

Bruce had put corporate interests and deleted it, I had already put
in person's

interest. We have to talk about a person-focused approach for all
of this. We

have to talk about persons, about the identity of persons, about
the security of

persons, and about the rights of persons.

And the two issues there are how can we ensure the
confidentiality, integrity

and availability of computer data and systems. And I think that
that covers

many of the things. That includes also the protection of personal
data, and how

can we do that in a global environment? Because our rights are
currently

protected by our constitutional nation state, while we live in a
global network

or Information Society. And we have to find a way to handle that.

>>MARC ROTENBERG: Thank you.

Mr. La Rue.

>>FRANK LA RUE: Yes, I think we have to have that human
perspective of

guaranteeing security and privacy to guarantee the openness, the
access to all.

But fundamentally, this means to have a human rights perspective
beyond the

technological development, the commercial developments, the
interaction of all

these elements is from a human rights policy and perspective which
will

guarantee that we will focus on human beings and their benefit.

>>MARC ROTENBERG: Dr. Hashem.

>>SHERIF HASHEM: I guess from what we heard from the panelists,
and I think

the issues that they raise are very valid, I think the IGF should
focus on

inclusion and empowerment of the society when we discuss issues

relating to

security, openness, and privacy.

And this can be done only through partnership and openness.

Encouragement of

the society. Different stakeholder to participate, and being understanding of

the other's views and trying to reach what is best for our society rather than

what is best for a special interest group. I think that will be a fundamental challenge.

>>MARC ROTENBERG: Thank you.

And finally, Minister Matic.

>>H.E. MS. JASNA MATIC: A very difficult question, I think, for all of us.

This absolute openness has created a situation that is entirely new to all of

us. And I think the biggest danger is how to use this openness in order not to

create more leverage for the already powerful ones. As when you have one voice

out of 6 billion, it is almost the same as you don't have a voice at all,

because who will ever notice it?

And it is a big issue, in my mind, to use that correctly and to empower

communities and to let them voice their concerns.

>>MARC ROTENBERG: Thank you.

Well, this is very interesting to me. We are all gathered here at a major

international conference on the future of the greatest technological revolution

of our era, and it seems that most of our panelists are primarily concerned

about the rights of people. So watch out, technology. We are looking at you.

Our audience now, you are invited to participate.

We have microphones at the front. We have handheld mics at the back. I will

try to recognize you in order.

I will ask you to try to please address a brief question or comment to one of

our panelists.

Yes, this gentleman over here.

>>STEVE DELBIANCO: Thank you. Is it on? Thank you. Steve DelBianco with net

choice. A few people stalked about privacy as a fundamental right for an individual. So my question to each of you would be, are individuals allowed to negotiate away that fundamental right? Because I think about what Mr. Alhadeff said, is we should optimize the way this works. And the optimum configuration for some people -- my teenage sons, for instance -- is that they may want to give away some of their privacy rights. That is to say, to let ads that are targeted to their interests show up on their applications, because they want to continue getting for free services like Facebook or Gmail or Twitter or Flickr. So should they be allowed to negotiate away what you are trying to establish as a fundamental right?

>>BRUCE SCHNEIER: I don't mind starting. I think your son would probably sell his kidney, too, because the money would be sure worth it. There are limits to what should be traded in terms of fundamental rights. We have to be very careful about giving rights the same economic status as you do other things.

So I think privacy should be a right and not a commodity. And while there are -- well, the stuff around the edges, basically in some instance the answer is no.

>>JOSEPH ALHADEFF: I mean, I think you have concepts of what's a right and what's control over certain types of information. And I think you have to start drawing fairly fine lines around how you define those things, because I don't think we want other people making decisions for us. But on the other hand, there are populations where you may want to take certain protections against them.

People who aren't familiar with the Internet may actually not understand what's going on. Older people -- That would be older people, not -- 13-

year-olds know

much better than 80-year-olds, in most cases, what's going on with the Internet.

But those are the kinds of things that have to be factored in those

decision-making processes.

And then I think one thing we always have to look at is when people start

making rules in those spaces, they have to look at what are the compelling

public-policy needs and how to make sure those rules are narrowly tailored. So

if there is a specific effect that you are trying to protect, that you manage

that effect and be aware of undue consequences for scope creep in the other

direction of controlling too much what an individual may choose.

>>MARC ROTENBERG: So we have a question from a remote participant. How shall

we handle this? Can someone ask the question on behalf of our participant?

Thank you.

>> Okay, sir. I have a question from a Ms. (saying name) in Brazil. And the

question is directed to Ms. Malhotra. You have raised for sexual rights and

human rights linking it with gender. Privacy and freedom of expression.

Unfortunately, your presentation was too fast for interpreters and the

transcription. I would like to ask you to back on the topic of the link between

sexual rights as human rights and the lack of a deep discussion on privacy and

freedom of expression.

Here in Brazil, it is an issue that is getting more relevance in the debates on

content regulation and law enforcement. There are clear contradictions which

lessons we can get from the examples you brought. Which lessons can you get

from the examples we brought?

How to advance in a more robust debate on freedom of expression, privacy, and

sexuality as you raised?

>>NAMITA MALHOTRA: I apologize for the speed at which I spoke.

I think, also, there is a connection to what has happened in Brazil in relation

to the child protection law and what it has been used for. And in that context,

I would like to reiterate the story about how the Indonesian law on pornography

is used basically to limit how women are controlled or how women -- how they are

allowed to participate in the public sphere.

In terms of what you are saying or asking in terms of solutions, in interprets

of privacy, there is what I had already raised before in the context of

contextual integrity of information which actually deals only with the idea of

data aggregation, that corporates can take your information and that when put

together, that can provide a huge amount of information regarding you or that it

can provide a huge amount of information regarding a community.

And in that respect, maybe one of the ways forward would be to think about

contextual integrity of information; that information that you give for a

certain purpose cannot be used for anything else.

There is debates which I may or may not agree with about using the notion of

consent about privacy as to -- and that is directly linked with ideas of

sexuality, because consent and not giving your consent forms the bedrock of most

sexual offenses, and also that the state criminalizes unnatural sexual acts

between consensual adults, say in the case of sodomy in India until recently.

So that might be also a way to go forward, to look at whether consent is an

important legal tool, whether it is more legally protected in other contexts

than privacy. Because privacy also has very low -- is not as well protected in

certain countries, like India where it's read into the right to life. It's

lesser than the right to health. So it's actually part of like a whole range of

rights. It comes above some, it comes below some.

So it is kind of not what could be called a very strong right.
So maybe consent, since it is also the bedrock of criminal law as well, might be an interesting way to go forward.

>>MARC ROTENBERG: Thank you.

Our next question.

Yes, here in the middle.

>>CHINELO: Good afternoon. My name is Chinelo from Nigeria. And actually, I

had two comments to make. I wanted to make a comment to the -- my colleague,

the gentleman over there that talked about trading rights and for privileges. I

just wanted to remind us like the panelist did that human rights are

inalienable. They can't be traded. I don't think that -- I don't know, I don't

think that should be a way that we can go forward.

And then I had a comment to make about the question of what the real challenge

is for the future of the Internet. And I think that a very real challenge, in

my mind, is crime overrunning society.

That's crime, e-crime, cybercrime, overrunning cybersociety.

We have many points of view, and we've come up with many concerns and all of

them are real, yet we have to make an analogy with -- analogy of cybercrime or

cybersociety with the real society, and try to be sure that we can catch up with

the cybercriminals, because they're going in leaps and bounds ahead of us, and

we have to be sure that, you know, this is a new frontier that we're dealing

with right now, and in order not to get to a place where we're like the old --

you know, the wild west or whatever you wanted to call it, we have to be -- to

try and run with them, or at least, you know, be side by side by them so we can

prevent it before it destroys the cybersociety. You know, those were my

comments.

>>MARC ROTENBERG: Cristine?

>>CRISTINE HOEPERS: Yeah. I think as I raised cybercrime in my speech, one of

the things that we deal a lot in Brazil, CERT.br actually don't do investigation. We are not police, so we don't actually investigate crimes, but

we deal with people that are victims of cybercrimes, frequently. And most of

the time, what we see is there is a mix of the victims. They don't actually

understand how that is perpetrated and the technology is making it very easy for

the cybercriminals to pose as third parties, to subvert the technology, to

insert and mix with the Web, and they even show fake pages to the victim and

they are really thinking that they are doing the right transaction, be it in an

auction, be it in exchanging information with someone. And I think the

challenge goes, as I said before, for the future about what exactly do we need

to do.

What we see is there are a lot of people overreacting and we need them to

control everything, to gather more data, and actually to just get information

about everything that is done online. That will not help either because no one

will be able to go through that information timely to fight cybercrime. So I

think it's a mix of having better software and technology and, in a way, having

people to understand better the technology that they are understanding.

The other panelists said something about 13-year-olds, they know technology

better than 80, but I have some nieces and nephews in that age, yeah, they

dominate a lot, but they don't understand how does it work, the SLA between

Google and them. When they use gmail, the data is not there. Why everything

they put online stays there. So the whole thing I think actually is people

don't understand the thing about trade, and I don't think that we should trade

privacy and trade this right.

So I think, yes, cybercrime will be a big -- really a big issue,

but we need to

think about. What is the fundamental thing we can do to actually cope with

that?

One of the things would be, yeah, to exchange a lot of information to make ways

about investigations to get quicker, but we cannot actually do that undermining

the rights and privacy and doing something bad.

So I think it's really a challenge about what is the good security measures

versus the measures that look like they're good, but they are not.

>>MARC ROTENBERG: Thank you. Mr. La Rue, did you have a comment?

>>FRANK LA RUE: Yes. Fully agreeing with my predecessor, I'd like to answer

two questions.

One is, I think we should never think of the possibility of limiting human

rights or we cannot barter our human rights or we cannot even talk about stages,

in terms of technology going first and human rights attaching up later.

I think we have to be very clear that it's the full exercise of all rights that

will guarantee advancement in all levels, especially as a democratic society.

But in terms of the biggest challenge, I really believe that the biggest

challenge beyond all the others -- there's many, but -- is accessibility. We're

talking about Internet as the global communication tool, but we have to make

sure that it becomes really global. That everyone has access to it. That it

does not become the limitation of the few either because they can't afford it,

as I said, or because of the technological sophistication.

I think all countries of the world need to develop this, all peoples around the

world.

I keep saying this, that before, freedom of expression and communication were a

civil and political right, but now they have become an economic and social right

because there cannot be development without communication.

>>MARC ROTENBERG: Very good. Thank you. We have a question

here, I believe.

>>LISA HORNER: Thank you. I'm Lisa Horner from Global Partners and Associates

and I just wanted to comment that it's very refreshing to hear about the

positive dimensions of freedom of expression from a number of our panelists,

especially from Mr. La Rue.

And the ways in which the human rights framework actually specifies how we can

balance between different social goods and rights, such as privacy, security,

and expression.

I think within the IGF, over the years, human rights have been presented in an

increasingly negative way, focusing, for example, on how we have to have less

expression and more security.

In the first IGF, we had a whole session dedicated to openness and freedom of

expression was on the list of subjects recommended by the MAG for discussion.

But now we have a session that's focusing on balancing different rights, and

freedom of expression isn't on that list. Instead, we have enabling networks of

freedom, which have tended to receive less attention.

So I'd just like to ask our panelists what we can actually do practically to

ensure that human rights standards are better included within everyday Internet

policy-making, and so that they are made to be the primary norms which underpin

Internet governance processes.

For example, is there a role for better coordination between the U.N.

organizations that have responsibility or are involved in different elements of

Internet governance? For example, between the U.N. human rights organizations

and between some of the other U.N. organizations, the ITU, WIPO, et cetera,

involved in these different elements of Internet governance, and indeed

coordination between those bodies and other private spheres and actors? Thank

you.

>>MARC ROTENBERG: Thank you. This is a very important question, how to incorporate human rights in the structure of Internet governance, and perhaps what I could do is ask the panelists if they could make a specific, concrete proposal for how to move this forward. Maybe Mr. La Rue?

>>FRANK LA RUE: Yes. I think, number one is that all the development has to be based on the knowledge of human rights and on the exercise of human rights, and this ultimately becomes the responsibility of the state.

Here's why I say that we don't have to see regulations in a negative way. I think that this has to be a development organized by the state, but in satisfaction and in the demand of the exercise of human rights.

A human rights approach in all the policies that are established by the states and, as well as those that develop the technology and the new techniques.

>>MARC ROTENBERG: Do any of our other panelists have a comment? Again, a specific or a concrete suggestion? Yes, Mr. Seger?

>>ALEXANDER SEGER: Thank you. We have been discussing often about the notions of what is cybercrime, what is cybersecurity, et cetera.

I think there is one advantage in approaching something as cybercrime rather than information security or threats to cybersecurity, because the moment you talk about "crime" you automatically talk about rule of law, you talk about conditions, safeguards, rules of procedure, et cetera. And I think as we approach the issue as an issue of cybercrime, it will automatically take into account basic safeguards.

Thank you.

>>MARC ROTENBERG: Thank you. I know we have many more questions in the room and we will get to you, but I'm also very pleased that we have people who are following the conference on the Internet, following the discussion, and sending

in their questions as well, so I will, on occasion, turn to some of these

questions that we've received from our online participants.

This one is from Miguel Alcaine from El Salvador and he asks the question: Why

haven't we discussed anonymity? We've talked a lot about privacy, but he says

there is a difference between the right of privacy and the right of anonymity,

and I'm wondering if any of our panelists would like to address this.

>>BRUCE SCHNEIER: I'm happy to make some comments. I think anonymity is very

important, especially if we're looking at the rights of the individuals with

respect to society. Anonymity is important even before the Internet, and it's

important that the Internet preserve anonymity, whether it's social or political

or economic. It's fundamental for all these things.

Actually eliminating anonymity on the Internet is very, very hard. You really

cannot design an Internet architecture that doesn't permit anonymity. Just

having something as simple as anonymous re-mailers, even in a perfectly

identifiable system, brings back anonymity.

So I think we need to recognize that anonymity is a social good, a political

good, an economic good, and it's a fundamental property of the Internet.

>>MARC ROTENBERG: No? Okay. Oh, Joe, yeah, go ahead.

>>JOSEPH ALHADEFF: Yeah. I want to build on Bruce's comment, because I think

the problem is sometimes people talk about only privacy and either full identity

or anonymity, and they don't talk about what's in the middle.

And selective disclosure of identity as appropriate for the needs of the

communication or transaction you're involved in is also part of the solution,

because you don't need to actually disclose all elements for all transactions.

There can be a selection of what is appropriate in terms of you may even have

pseudonymity for certain types of things, as opposed to anonymity,

so I think we

need to look at the broad panoply of tools that are available and not just

either think of anonymity or full identity as the only options that are available.

>>MARC ROTENBERG: Thank you. I know we have a person who has been waiting patiently in the middle here. Yes, sir.

>>VINCENZO VITA: Thank you. Vincenzo Vita from Italian Parliament.

Where is the shadow limit between security and censorship? The people of the

net is very sensible to this occasion. Like the operators of the connectivity

suppliers are targeted by some draft legislation to introduce filtering

resources agree that filtering is useless, and is even impossible. It's merely

one way of postponing a resolution to the problem. We have to organize, I think

-- we think -- ourselves in order to debate the problem. Also in Italy, we need

(inaudible) in Italy. Thank you.

>>MARC ROTENBERG: Any comments from the panel on the effectiveness of

filtering? Yes.

>>FRANK LA RUE: I think the limit between security and censorship is very

difficult to establish, but it has to be established, and one of the ideas is

that limitations do exist, in which security could be part of those limitations,

but limitations have human rights criteria to them.

They have to -- in any state, they have to be established by law prior to its

application, normally applied by the judiciary, not by any administrative body,

much less like it happens with Internet, applied by a private enterprise hired

by the state to monitor, to screen. That's not acceptable.

And thirdly, it has to be applied in the protection of a higher good, or a more

important issue, to protect someone else's rights.

So I think there are criteria in which are the legitimate limitations.

If it doesn't fall into that criteria and the state is applying measures, then it becomes censorship, censorship into the freedom of expression and communication of the people.

>>MARC ROTENBERG: Did we have a question on this side? Yes. Okay.

>>BERTRAND DE LA CHAPELLE: Good afternoon. My name is Bertrand de la Chapelle. I'm the French representative for the Information Society.

I wanted to add to the comments that were made, first of all, that it's a great pleasure to hear the reiteration that the privacy, openness and security are not necessarily contradictory, and anonymity or nondisclosure of names is a typical example where, in certain cases it can be a reinforcement of the security of the user, which is a case where both go together.

But I just wanted to drill down very briefly on the case of social media, Web 2.0, which is part of this agenda, to see how the elements that have been mentioned apply to specific words.

Social media are redefining some elements or asking new questions on privacy, freedom of expression, and even copyright sometimes and if we dig deeper on the privacy notion, it's about somehow introducing a redefinition of what intimacy is. Intimacy was usually what you do in your home. Now we are exposing a lot of your personal information voluntarily, and it is just bringing new questions that have to be addressed.

So how do you manage online intimacy, those people you allow to see things about you and those who don't.

And I just would like to share, on a personal user experience, the distinction that is naturally felt between the data that I selectively disclose, as Joe was saying, the data that I can give to one site or the other, when my concern is that they are not necessarily mixed or cross-analyzed; the type of

data that I publicly make available voluntarily, either completely or selectively on a Web site like Facebook or user-generated content like Flickr; the data that some companies collect about me without me really knowing their details, and the data that other people post about me, like tagging me on a picture or making a comment on picture.

I just would like to highlight that one of the benefits of the IGF is that it allows to sort out some subthemes, sub-subjects, as an application of the general principles that we've adopted, and I hope that the -- some of the workshops that are continuing will dig deeper and explore those elements.

And the last point is, when we talk about the governance of social media, there's the external governance, the international treaties, or the national laws, but there is also the laws that are developed somehow internally by those large networks in the form of the terms of service, or terms of use. And the way those terms of use are being used and the kind of complementarity they do between the protection of privacy and openness is also an issue that has to be discussed those networks are transnational and it's important to see how the terms of service evolve. Thank you.

>>MARC ROTENBERG: Thank you for this comment. This is an interesting question about social media and intimacy. Would someone like to speak to it? Yes.

>>NAMITA MALHOTRA: I kind of agree with you, and I think I'd reiterate what a lot of people have said about trust, and being online being a lot about trust. In fact, one of the things I said about the net is that it's about friendship, and that's the cyber-- original social cyber form, that we trust each other and friendship is the basis on which we proceed, whether it's Facebook

or Orkut or

anything else, but as you pointed out, there is three different kinds privacy --

or private data that you're talking about, what you give to the corporates, what

you share with each other, and what someone does with your own data. So these

are very different things, which, again, the idea is that you give out the

information in different contexts and they should be limited to those contexts

and used only within those contexts.

But, again, I think -- and just to be, I don't know, a little fuzzy about it,

it's actually quite endearing how humans are able to share so much information.

It's actually a very nice trait about us, that we put out so much of ourselves

online and we do it so willingly, trusting the community, trusting society to

not disclose or to use that information wisely. But unfortunately we do live in

a world where the state picks up on certain aspects of what we put out there, or

corporate entities, rather, pick up on certain bits of information that we put

out there, and then because it is complicit with the state, shares that

information with the state, which then results in negative action such as

arrests or just harassment or censorship or banning.

>>JOSEPH ALHADEFF: Well, I think you have to think about a couple of issues,

and to the point that was made, there's a lot of work going on related to

use-based models because there is the concept that some information has gotten

beyond the scope of notice and consent and when it's beyond that scope, how do

you think about a use-based model to help protect that information?

So there is research on that, and practical things looking at those models that

are being developed.

I think the other thing you have to think about -- and I'll take Bertrand's

examples and add one, which is, I think, more complex and difficult

to deal

with, which is the picture you take where the subject matter isn't the problem

in question, it's something in the background.

Where it's a third party that was caught in the background. And the question

then becomes, you know, where is the responsibility to that person in the

background who happens to be in a public place where you've taken a picture of

someone you know? Both the photographer and the main subject are consensually

posting this picture. And I don't know the answer to that one but that -- when

I've been thinking down those lines, that's the one that stumps me most.

The last thing I would say is, as you think of some of these issues and you

think in the context especially of social media, I think one of the things that

has been most amazing in this is that social media have also have a democratizing potential in the sense that the community itself has risen up

against terms they don't like and has been the single most effective thing to

change them, and that's been just an amazing thing.

I mean, the Internet had that as a portion, so I remember there was a -- there

was a Web site that had sold some goods, they hadn't done -- they hadn't done a

great job. When you looked on search engine and you typed in the name of that

vendor, the first thing you found out were complaints related to that vendor.

So that there was this information exchange that was occurring. But that's

really a small scale compared to a change in terms of reference yields 80 or

100,000 people spontaneously acting in a truly short amount of time because the

medium itself has enabled them to make those comments.

So I think there's -- there are some self-correcting features that don't deal

with the fact of whether or not terms and conditions are clear and all the other

kinds of issues. But the media itself is part of the solution in

some of these cases.

>>MARC ROTENBERG: Thank you. I know we have many questions. We'll try to get to everyone in turn. I'm going to this woman here, please. Thank you.

>>THOMAS SCHNEIDER: Thank you. My name is Thomas Schneider. I'm working as the Information Society coordinator for the Swiss government.

I have two questions or remarks. The first one is with regard to this growth of so-called free services that you do not pay directly through a fee, but you pay indirectly through being profiled or other hidden costs that you might incur indirectly.

And the question is: Don't you think that -- or the question is: To what

extent do you let users choose whether or not to use these services? Especially the ones that do not have the money, that do not really have a choice to choose services that are of a higher quality but they have to pay for.

So the question is: Is there a risk that there is a -- we're getting into a two-class society, where the rich ones have the resources and the capacity and the education to protect themselves, their rights, and the poor ones that want to be part of that Information Society do not have the means to protect themselves?

In the Council of Europe, some experts talk about outsourcing human rights from the responsibility of governments to private sector services, which creates a problem because the liability is not clear anymore. This is the first question.

The second question is -- or remark is with regard to involving human rights experts into the structure of Internet governance. There was an answer by somebody that this should be done by the governments, that should defend the human rights or the rights of their citizens. In my experience in working in

the ITU and in ICANN and in other bodies that deal with so-called technical questions, that take technical decisions with regard to telecom and the

Internet, there are not that many human rights experts in governments'

delegations because normally these are people that know about the technical aspects of these decisions.

So I wonder how you see that governments should defend the -- these aspects in

these organizations. And in my view, it's -- the only thing that works is that

stakeholders are involved and can exercise pressure on governments to make sure

that kind of the holistic picture of the whole society interests are represented

in these organizations. Thank you.

>>MARC ROTENBERG: Okay. So thank you for this comment, an important reminder

that it's not only governments that provide human rights expertise in

policymaking but the actual stakeholders.

The question goes to the so-called free services, and the various ways people

are asked to provide personal information and other details to get access to

these services and whether this creates really a two-tiered economy, or --

there's views on this. Bruce?

>>BRUCE SCHNEIER: I can address the first one.

I mean, this notion of cross-subsidies isn't new. I mean television is an old

example of that. There's no way to charge for it directly so advertisers were

brought in, and the customers of television were, in effect, the product that

was being sold to advertisers.

And that's no different from Google.

So I don't think we can get away from cross-subsidies. And instead of it

making a sort of a two-tier system of haves and have nots, I think you end up

with a one-tier system like television where everybody has to deal with that. I

mean everybody uses Google, everybody watches television.

Everybody in the

United States has to buy cell phones with calling plans attached to them. I

know it's different in other countries.

So the only way forward, I think -- we can't get rid of them.

It's very hard

to regulate them. But if we have accountability and transparency, what we've

been saying on stage for some of these other things, I think it's the only way

to make that palatable to society.

Cross-subsidies aren't going away and the Internet makes them very, very

powerful because there are a lot of things you can give away if you sell

advertising and the market for that is going to change. We're already seeing,

you know, Google's ad words, the revenue goes down considerably because they're not

-- they're less valuable but I don't think we can stop that. I think we have to

make sure that it's explicit, transparent, and people know what's happening.

>>FRANK LA RUE: Maybe a quick thing is also who are the actors.

If you really

want a human rights focus and the appropriate focus, you want the -- the public

authorities to learn about how many rights, which all states should have

specialized people, especially in the level of communication. You want those

corporations that develop the technology to have some of their staff specialized

in the human rights perspective, but you also want the users and associations of

users to be aware of their own rights and the exercise of their rights, but I

think you should bring in a fourth actor, which is the NGOs, the specialized

NGOs in human rights that are already experts on the subject.

There could be --

there could be a four-way dialogue that would guarantee this future perspective.

>>MARC ROTENBERG: That's very helpful. Thank you. Yes, right here, please.

>>ZAHID JAMIL: Thank you. I'm Zahid Jamil from Pakistan. I'm an

attorney

from there. And I want to thank Namita for bring to the fore the subjective and

arbitrary language in some national legislations with regard to cybercrime in

several countries that are coming out. This is the problem with national

legislation. I've been hearing about national legislation as a solution,

probably. The problem with national legislation is it's made to be disharmonious with the global legislation scene, and free speech

for one may be

incitement of violence for another.

And so in Pakistan, to give you an example, what we did was we used an

aggregator, as you mentioned, a business aggregator like YouTube to basically

lobby and advocate against cybercrime legislation which was contrary to human

rights, et cetera.

Now I mentioned this, actually, two years ago. What is good to report is that

because of that advocacy, which is on YouTube, legislators and many others in

the country picked it up and actually were led to the reversal of the

legislation -- I'm sorry. Sorry. Slow down.

I'm sorry. I'll go back a bit. What was good about that entire exercise was

that the entire advocacy came online on YouTube, and legislators picked it up,

media picked it up, and it became a whole advocacy that the entire civil

society, as well as business, started lobbying for and against.

And the

legislation has been sent back now from the National Assembly to the standing

committee for comment. So that's one way that you can actually use businesses,

which are democratizing tools, on the Internet.

But my question, basically, is, Namita, to you. You said that sometimes

businesses are complicit with state or law enforcement agencies, so taking the

example of what happened to YouTube in Pakistan, where there was some material,

some video which was supposedly against the -- the census of certain people in the country so they actually blocked it, that led to internationally and globally YouTube coming down. Now, what does a business do in that situation, because there's national legislation that they're going to be impacted by, so I don't know about how we would sort of define that as complicity, but maybe it's just something they have to do and they're forced to do. Otherwise they go to jail or their business suffers. So that's my question to you. My second question is, and this is for anybody on the panel, somebody mentioned the important role of the WTON, international governmental organizations in the IGF structures. Well, does the existing Budapest convention, which is the only convention on cybercrime, have a role to play in bringing human rights, due process and safeguards into the structures of Internet governance? Thank you.

>>NAMITA MALHOTRA: I think what -- Though I kind of understand the story that -- the little that I caught of it, but I think what I would differ on would be the fact, this idea that businesses would suffer. In fact, we are talking, at least when I talk about global corporations, you are talking about very big corporate entities that have a lot of power. So I feel it is, in fact, up to these corporate entities to have some kind of moral or ethical center. Whether it is Google telling, say, China that I am sorry that we will not block or filter certain Web sites that turn up in the search, it is actually unfair to see businesses as victims of national or even international legislation because they are so powerful that they might even be shaping these legislations for their own purposes. So it is maybe interesting to, in fact, look at it the other way and see what is the role that these businesses are playing. And maybe -- And

maybe the

complicity that I talk about may be both ways. It is also be about the state

but it is also about global corporations and what they do. I don't know if that

answers you.

>>MARC ROTENBERG: There was also a question on cybercrime. Does anyone want

to speak -- Yes.

>>ALEXANDER SEGER: Thank you. And by responding to that, perhaps I will also

partially respond to one element of the question that was raised by Thomas over

here before, and the point I made earlier. If you talk about information

security, you talk very much about a technological problem that you have to

address one way or the other.

If you talk about cybersecurity, you also talk about a technological question

or a defense question, in many ways.

The moment you talk about cybercrime, you talk about criminal justice, and with

that about safeguards, et cetera.

And at the Council of Europe level, we, indeed, have developed the Budapest

convention on cybercrime which proposes a proportionate and appropriate response

to that. And I would appreciate if all of you also, when implementing the

convention on cybercrime, which I hope you all do, also take seriously Article

15 about conditions and safeguards, which is essential there.

What I would also like to update line, the experience we have had in many

countries; namely, that we have been working with countries about cybercrime

legislation to start with. But very soon governments came back to us and said,

well, we have a problem from the community, in parliament, from our people. We

have to find some safeguards there. And very soon we have started to then work

with governments about data protection and privacy legislation.

So that shows that it's built into the process.

In some countries, this process has taken many years. If you take

Brazil, I think after 12 years of discussion about cybercrime legislation, you are now starting all over again.

I think this shows that there are some safeguards built in also from the community.

>>CRISTINE HOEPERS: That is like the third or fourth time someone talked about Brazil and cybercrime, so I am jumping in again.

One of the things is I think we started discussing a cybercrime law in '97, so

1997. I think as that law went to the Congress and back, and people were

discussing, there were a lot of people putting things in the law that would

undermine a little bit of privacy. Then that went back and forth and back and forth.

And what happened now is that it is in the last phase in the Congress, they get

out of the law all the questions that were raising questions about privacy, so

the law is getting simple. And I think this is what they are doing now, trying

to not actually touch the points that were raised that they were good to fight

cybercrime, but they could undermine privacy. So that was all debated in Brazil.

So what the Congress is now doing is taking these things off the table and

trying to focus more on what is not polemic about privacy.

And there was a question before about how Malhotra could give examples to

Brazil, and some people raised to me that on Wednesday, 11:30, there will be a

best practices forum about child pornography, and there will be people from

Brazil there talking about best practice and how to fight child pornography in

developing countries, so that could help people interested in more that line.

>>FRANK LA RUE: In the question of what happens when you have sort of a

contradiction between losing market or defending human rights, and

I think that
it's very clear, and has been said by the panelists, that there is
no
contradiction. You can never give in human rights.

I heard in some moments, in some panel in this conference, that
first you
develop the technology, you create the network in a new country,
and you bring
up-to-date their possibilities of communication, and then slowly
you bring up
the issue of human rights and persuade them. It doesn't work that
way. It
works the other way around.

First you have a human rights commitment. You strengthen
democracy and
democratic principles and then you bring up the technology.
Otherwise, it will
never work, and it is a self-defeating point.

I think you can never leave the human aspect of respect beyond the
technological aspect.

>>MARC ROTENBERG: Dr. Hashem.

>>SHERIF HASHEM: Well, the matter of setting up regulations, I
mean within
the legal framework of a convention, taking sort of actions that
would reflect
on the way the society uses the technology, the Internet in this
case, has to
involve different parties in discussion, different aspects of it.
Where to go
about it. How to criminalize certain acts or not and to what
extent you punish
the criminals.

In our case in Egypt, we have involved different organizations,
different
stakeholders. Experts, legal experts, technology experts,
companies, and they
sit on the same table and discuss these issues. Because you cannot
rely on
really a cascaded process where you set up the regulation and try
to convince
the civil society to adopt it. You have to include them in the
process. And
that has worked beautifully in many of the legislations -- I mean
especially in
the child protection law that we passed last year or even the
technologically

oriented legislation like the e-signature law and the telecom law.

So if you involve society, the process would be longer, but you end up with

something which is acceptable by almost all stakeholders.

>>MARC ROTENBERG: Very good. Over here, I know the gentleman has been

waiting.

Yes.

>>JEAN-MARC DINANT: Jean-Marc Dinant privacy expert for the -- Okay.

Jean-Marc Dinant, privacy expert for the Council of Europe, and also (inaudible)

at the University of Namur in Belgium.

I want to come back to the questions of privacy negotiation, because I believe

it's one crucial issue now on the Internet.

Let's imagine that for entering in a supermarket, you have to execute a short

dance and say, "I love the supermarket. The supermarket is wonderful. I like

to buy in this supermarket." And if you are not doing it, you cannot enter in

the supermarket. In fact, it will be mandatory to sell your freedom of

expression.

So the problem is that there is something very strange.

We have the false impression that the Internet is free. But when you speak

when the cyber marketing industry, you understand that there is a price to pay

to go on the Internet, and the price is privacy.

And furthermore, marketing say, okay, thanks to us, the Internet is free. But

who is paying the marketing industry?

The marketing industry is paid by the companies. And who is paying the

companies? The customers.

So, in fact, the customer is paying twice. Is paying by giving his privacy and

paying a second time to get a higher price for the same product.

I want also to come back on the questions of intimacy. Intimacy means, in

fact, confidentiality.

If I'm reading a newspaper, the article that I will read on the net is a story

between me and newspaper. But who is aware about the fact that,

for instance,

Google and ethics, following a survey by the Berkeley University in U.S., is

present on 88% of the Web site to Web box? It means that for the man in the

street, its traffic data is stored somewhere in the U.S. on the Google, data

(inaudible). Who is aware about that?

And finally, I believe it's very dangerous to try to negotiate the privacy.

Because if you want to negotiate your privacy with a big company like Google,

you will not be able to do that. Negotiation of privacy for me means privacy

for the clever and for the rich.

>>MARC ROTENBERG: Thank you. Well, you have asked a series of very

interesting questions. And if I can be permitted just one intervention, as the

moderator, with respect to a privacy issue.

I think part of the confusion in this area may be the view that individuals

face a choice only to keep information and thereby keep their privacy or

disclose their information and thereby give up their privacy. And in my view,

this is not the right way to understand it.

I think the right way to understand it is whether their information will be

disclosed, protected in law, used for an appropriate purpose, not exploited, and

respected, which is a disclosure that occurs in the context of a legal

framework, or whether their personal information is obtained and used for

whatever purpose the business that obtains it chooses to use it for.

And it's actually this choice that I think is arising increasingly for the

Internet. Whether we are able to ensure privacy where information is disclosed

paradoxically, or whether we say that we won't ensure privacy where information

is disclosed.

I don't know if my panelists agree with this view or not, but in many areas it

turns out to be one of the most important questions, I believe, for Internet policy.

Is there any comment?

This seems to be sufficient. Okay. Thank you.

Let me go in the back, then.

>>STEPHEN LAU: I'm Stephen Lau from Hong Kong.

Marc, actually, in his interim conclusion after the presentations by the

panelists, he was mentioning about when we have the greatest technological

evolution with the Internet, the issue is more about protection of personal

values and personal data protection.

So I'd like to make two observations. One is on the personalized kind of

basis. The other one is on the technology.

My good friend Joe was talking about the biggest challenge in the near future

of Internet or foreseeable future of Internet is trust.

I think when we talk about trust between government and its citizens,

corporation with its employers -- its employees and customers; however, nowadays

it goes beyond that because once you put your personal data out on the net, you

can be sure they will be kept forever. You can be sure that it will be used,

copied, forwarded, used inadvertently or otherwise by design. And the worst

thing is you basically trust, you don't even know who -- which entity some point

will be using your data.

And the sad thing is the entity that uses your data may not even know that it

is actually infringing or using your own data.

So I think as far as on a personal point of view, the biggest challenge, and I

hope the governments and the civil societies, in terms of self-protection, it's

the education upon which that if you, whether you are a teenager or you are a

senior citizen, that if you use the net, then you better make sure that you be

aware of this danger.

I was looking at the title of this conference, Internet

governance, creating
opportunities for all, and I thought that in this kind of education
for using
the Internet, it could read the first course on such, 101, would be
your

Internet: Creating your data for all.

So the second point is about the challenge as far as technology is
concerned.

I was at a lunch discussion yesterday when the Minister from
France was talking

about initiating an initiative regarding your right to oblivion.
It actually

goes beyond the right to anonymity. It actually talked about your
right to be

deleted as far as your personal data is concerned.

So my challenge to the technology -- to the technologists, the
pioneers,

including of search engines like Google and other really brilliant
algorithms

created for search engines whereby when you put in a couple of key
words and

within a couple of seconds, you would have hundreds of thousands or
even

millions of synonym related information that is supplied to you,
and with that

maybe hundreds or thousands that are really of relevance to you.

So it is possible to have personal data cast into oblivion,
deleted by putting

in, like, say, a photograph I wish to be deleted, my own. Putting
it into the

net, within a couple of seconds, like we get our search engine, our
information,

have them all deleted.

Thank you.

>>MARC ROTENBERG: Thank you, Stephen.

This is an idea that is actually becoming popular, the ability to
delete your

history, if you choose to do that.

In fact, arguably, the recent campaign involving the change in the
Facebook

terms of service was very much about that issue. Because as you
know, many of

the Facebook users objected to a change in the provisions which
appear to make

it more difficult for people who chose to leave Facebook to be able
to delete

their account.

So not only at the theoretical level but also at the practical level, I think

this is something that's of interest to people.

So let me ask the panel, the technologists, is it possible that we could, in

some instances, delete our histories?

>>BRUCE SCHNEIER: I can start. Technically, no. And you know that's true

because you could have a copy of the data on a DVD in a file cabinet, and you

just can't go in and erase that. It's nonerasable media, for heaven's sakes.

But you can do it through legislation. If the issue is Facebook not deleting

our data when we ask them to, all it takes is a law saying you have to do it,

and then companies will follow.

For a lot of these problems, there aren't technical answers, but there are

legal answers. And that's really where we have to look when we move forward,

with things like our data is used, how it's stored, how it's bought and sold,

how long it's saved and how it's deleted.

>>JOSEPH ALHADEFF: Thanks. I think, Bruce, the concept of the company is

perhaps the low-hanging fruit, because the problem is if it was posted, it may

have been copied, it may have been downloaded, it may have been transferred and

then the question is you may have deleted the source, but can you delete the

tail after the source. And that's perhaps the more complex question which I

would defer to you if you have an answer because this is more your remit than

mine.

>>BRUCE SCHNEIER: The answer is no.

>>JOSEPH ALHADEFF: But I did want to make a comment on Stephen's point,

because it also goes to your point of are there other ways to address this

issue. And Danny Weitzner and Tim Berners-Lee and a couple of other people that

I apologize that I forget their names, collaborated on a paper on

accountability

while Danny was still at W3C. And it was a very interesting paper that started

laying out use-base models because the premise of the paper is there are certain

types of information that have gone beyond the level of user control because

it's no longer part of the bilateral relationship. Which is part of the

question you posited in the first part of your question.

So when we start looking at those issues, use-base models become important

concepts on how to look at those issues. And they are not a silver bullet.

They don't answer all the questions. But they are an interesting first step to

look at in these contexts.

The other thing I think we have to think about is education in this space.

Because it's nice to say that teachers or parents or companies can try to

educate people, and by all means they should. But they are not necessarily --

think of when you were back as a teenager. They are not necessarily the

audience you listen to most. They were occasionally the advice you avoided

first.

And so the question becomes what paradigms of education can we use, especially

in a situation where in some cases young people may know more than their

teachers about the technology they are discussing.

So again, how do we think about innovative ways to look at the educational

paradigm.

And this may go to something that has worked well in Egypt, especially in the

area of education, is the concept of a public-policy partnership. And perhaps

not just engaging government and business, but also civil society in that

discussion so that you actually can have a rich and perhaps an innovative way of

approaching these things.

And by all means, include kids in the discussion. Because from

marketing,

people have learned, focus groups, may be a good idea. Well, maybe the kids

have a little bit of information to tell us on how it's best to reach them.

So I think we need to be a little, occasionally, innovative in our educational

paradigms, too.

>>MARC ROTENBERG: Yes, at the back of the room, please.

>>RIKKE FRANK JYRGENSEN: Thank you. My name is Rikke Frank Jørgensen. I am

from the Danish Human Rights Institute.

So a lot of the comments we heard today speak to the importance of the human

rights framework as the point of reference. And also address the lack of global

privacy standards, those standards that elaborate a bit more on the quite

general provisions we have in the human rights framework.

So I have a question that addresses Mr. Frank La Rue mostly as to how we could

encourage or initiate a process to have a general comment on the right to

privacy to start with that would actually address some of these new issues that

we are discussing today. And in that way could help national policymakers and

lawmakers when implementing the right to privacy.

>>MARC ROTENBERG: Okay. So proposals for an international right to privacy.

>>FRANK LA RUE: Yes, and the idea of getting a general comment from a human

rights committee as establishing a standard I think is a great idea.

As a matter of fact, the human rights committee is looking at a general comment

on Article 19; again, or an update on a general comment on their Article 19.

But they didn't go as far to look at the limitations in general in Article 20, I

guess because they don't have common agreement on that view.

But I fully agree. And I myself will transfer this sort of request and belief

that this would be an appropriate moment for the human rights committee to

establish a general comment on privacy principles.

>>MARC ROTENBERG: Yes.

>>ALEXANDER SEGER: We do have at the Council of Europe level, for our 47 member states, a treaty which dates back I think to 1981 on data protection.

And it was recently decided by the Committee of Ministers of the Council of Europe that this treaty should be open to third countries. So here is a practical tool and existing instrument that any country that meets the same standards that are foreseen under that convention to join that treaty.

And I also mentioned earlier that recently there was this meeting of -- I think the 31st meeting of data protection Ministers, a meeting in Spain that developed some ideas for some global principles that could be followed by countries.

So I think there is -- There are some instruments available. There are some further ideas. But I think we have to push that further to, indeed, come to a globally trusted data protection privacy standard.

>>MARC ROTENBERG: I should mention also that in Madrid there was a very important declaration set out by civil society groups on privacy issues. And that Madrid declaration is available at the Web site of The Public Voice.

I think we had before, yes, someone in the back.

>> My name is (saying name) from Indonesia. I would like to mention that there are concerns about trust for accessing information through public facilities as CAP, or Community Access Point. There is a need for parents, teachers, to have trust when their student or child going to the public facility, or CAP, especially in developing countries, when CAP becomes the only access for information in rural areas.

In my point of view, government and society itself should also take on those concerns.

With regard to the positive uses of Internet, privacy, and so on, probably it

should be created a platform where each country set their criteria on ethical dimension and local ethic to which the positive uses of the Internet can be delivered and anticipated.

Thank you.

>>MARC ROTENBERG: Is there comments from the panel?

No comments? Thank you.

Thank you for the question.

Yes, in the middle please.

>>PAVAN DUGGAL: Good evening. I'm Pavan Duggal.

I am the president of Cyberlaw Asia and a practicing attorney in Indian Supreme Court.

Specific question to the panelists. Five broad game changers are currently happening. Number one, there is a huge explosion in the adoption of smart communication devices. And that is happening more so in Asia-Pacific, India and China.

Number two, there is a tremendous increase in the quantum and the quality of cybercrimes targeted against nations. Examples being that of cyber war and cyber terrorism in front of us.

The third, the emergence of the voice Web and the mobile Internet is suddenly changing the horizon.

The fourth, cloud computing is bringing up certain new parameters. And

finally, the fifth, social networking; more so social networking in the mobile space and on mobile platforms and communication devices.

Given these five broad game changers that are currently emerging, and more so

in the part of the world where Asia is located, I have a question for the

panelists. Does the panel look at some kind of paradigm shifts in how the issue

of privacy is going to be either viewed, addressed, or appropriately, shall I

say, looked at by national governments in the context of this entire smart

mobile platform and mobile devices?

On to the panel.

>>MARC ROTENBERG: Thank you.

So the question is recognizing these dramatic technological transformations in communications and computing, does this lead to a paradigm shift in our understanding of privacy.

Comments from the panelists.

Bruce.

>>BRUCE SCHNEIER: I can give a shot. I mean, I try to talk about a lot of

these things and the difference is that it used to be -- what I think of as a

fortress computer center, that if you wanted to be secure as a person or as a

corporation or as an organization, you would do it yourself.

It was very much like -- that you could build your own security. You could

build your own walls.

And what these trends indicate is that things are much more interdependent,

that we're losing control of our data, we're losing control of our employees or

even our notion of borders, with mobile computing and cloud computing and social

networking. And, yes, criminals are getting much more sophisticated, and I

think this, again, points to the need for broad legislation.

That we can't just rely on technology to provide security. That we need to

rely on others. And it gets back into what we were talking about, trust and

accountability. But I think it does point to the need for broad legislation,

and that will be the way -- the only way out of these -- the bad part of these

trends.

>>MARC ROTENBERG: Very good. Thank you. We have a question over here.

>>LIESYL FRANZ: Thank you. My name is Liesyl Franz, and I'm with TechAmerica,

an ICT industry association.

I'd like to talk a stab at answering the question Mr. Rotenberg posed to the

panel earlier about the challenges to the Internet.

I would like to say that I fear a challenge to the Internet is the imposition

of a regime or a set of regimes that would inhibit the ability of our technology providers to continue in the very business that enables the access, the services, and the innovation that so many people around the world are calling for.

You could say, then, that the greatest challenge to the Internet and the services that are provided by the virtue of its existence is that it no longer

be available, due to overwhelming constraints to its provision.

That may sound slightly like hyperbole, but I think in the context of

broad-reaching legislation or regulation or constraints, it's something we need to think about.

Some of these services that you have today and are relying on today would not

have been created if there had been an environment that prohibited them.

To address the various comments regarding corporate interests, then, along the

same lines of ensuring availability, companies do acutely realize and recognize

that it is in their interest to provide security, privacy, and dignity to their

stakeholder community. Their very customers and users.

I'm not saying that there aren't outliers to that philosophy, but I do think it

is important to recognize the efforts of technology providers to build security

and privacy into their products and services, particularly in the environment

that we see today, the increasing threat environment, the increasing economic

environment that we see today.

Given that, I think it's important to ensure an environment where industry,

government, and civil society can engage in dialogue, both here at the IGF but

also in our own jurisdictions so that we can continue to address the synergies

between privacy, security and openness and inform the discussion from each of

other perspectives and expertise.

We can't shut down that dialogue because it's so important to recognize where the strengths of each group are, and what the specific roles are of each, as Mr.

Alhadeff pointed to earlier in the session.

So I do have a question: How do each of you, in each of your roles, engage with industry -- and if you are from industry, please address that, too -- to help work together towards solutions? And I'd encourage you to address it a little bit more from the cybersecurity side of the equation, given that we've discussed privacy quite so much this afternoon, and I'd like to highlight the cybersecurity side, recognizing that the two are not unrelated. Thank you.

>>MARC ROTENBERG: Okay. So the question is: How do you work with industry primarily on cybersecurity issues.

>>ALEXANDER SEGER: Why are you laughing, Bruce? You don't like this question?

>>BRUCE SCHNEIER: No, it's a good question. It's a hard question.

>>ALEXANDER SEGER: I think the idea that government is there to control us, I don't like that idea. And I don't think it's a realistic idea. And I don't

think that the idea that industry is only exploiting us, therefore, we have to confront industry or cross them out, as you did, Bruce, is also not such a constructive thing to do.

I think we need the cooperative approach. We cannot, as I underlined earlier, we cannot deal with cybercrime without working with the private sector. It's not possible. And we have, for the past years, have worked extensively with industry. We have had private sector support to our cooperation activities in that area. We have been elaborating, for example, guidelines for the cooperation between law enforcement and internet service providers to help both sides structure their -- structure their cooperation, develop a

culture of

cooperation, and I think we have been -- we have been quite successful in that.

These guidelines are implemented in a number of countries where they are used as

a common agreement in order to organize such cooperation.

So indeed, in practice -- and it may not have appeared from the discussion so

far in this panel -- in practice, we do have a cooperative approach to this, but

at the same time, knowing that there are limitations of how both sides, law

enforcement, public side, and private side, can cooperate -- for example, we

have -- it is now accepted all over the world that law enforcement can receive

support from the private sector and needs support from the private sector for

training. At the same time we developed similar concepts for the training of

judges. There is more of an apprehension from the judicial side there. They

don't want to have direct private sector support because it could compromise

their independence. So we also have found a way to establish possibilities for

cooperation without compromising the independence of judges. So there are many

ways of dealing with that, and it's actually our daily bread and butter to work

with both sides, private sector, public sector, in this common undertaking.

>>MARC ROTENBERG: Dr. Hashem.

>>SHERIF HASHEM: Well, I mentioned earlier how we -- in drafting legislation,

we involved the private sector, and by this, I mean inviting them to be part of

the committees drafting the legislation. That happened in drafting the telecom

law, the e-signature law, and drafting data protection and privacy law in Egypt,

and that's how we included them early on.

Then when discussing the final draft, we involved the NGOs, the industrial

associations, so we involved a larger crowd of companies and got the feedback

from them.

At the operational side, our CERT, computer emergency response team, which is established at our NTRA, National Telecom Regulatory Authority, has open links with all the key players -- the ISPs, the GSM operators, even across different sectors, through the banking sector, the financial -- where we involved companies and what we are trying to do is getting them actually the right human resources, involving them in our training program. We fund the training of their professionals at the international level, have them get certified, so whether it is operational or the regulatory aspects, they are involved so they are not surprised by any move that we take.

At the same time, we get their feedback, because they are offering services to citizens, and that's very instrumental to get their feedback as we move on.

I'd like also to include that this happens in cooperation with other civil society organizations that would get us the direct feedback from the customers, the final citizens receiving the services.

>>JOSEPH ALHADEFF: I think there's a broad range of consultation and facilitation that actually already is occurring, and I would say the cybercrime treaty is a very good example, where both civil society and business worked with governments related to some of the terms in the treaty in its formative stages.

I think the encryption debate of a number of years back was another place where the dialogues were enjoined by all parties to a constructive and productive end.

I think fora like the OECD, where there is not just civil society, business and government, but also the technical community, is present and engaged in those discussions is another important way of bridging these gaps. So I think we have fora.

Does that mean that we agree all the time? Certainly not. Does

that mean

that, you know, heights always in a positive result? No. But now more so, I

would say, than before in lots of cases. And I think the concept of the

dialogue has matured. I think that's true in the IGF, where the dialogue has

matured significantly since its early days, or even since the WSIS process. I

think it's true in some of the other intergovernmental fora where some of these

discussions take place and I think it's true in the direct interchanges that

occur between some companies and some civil society organizations where there

are frank exchanges of views so there's a better understanding of the concerns

on either side.

So I would guess there is a productive path forward without necessarily saying

that we've reached any kind of, you know, permanent solution set, but I think

there have been some very useful bridges that have been built.

>>MARC ROTENBERG: Thank you. We're actually -- oh, I'm sorry. Mr. La Rue.

>>FRANK LA RUE: Quickly, I wanted to emphasize this dispositive notion that a

proactive dialogue and a positive dialogue between precisely civil society,

business and government or state could actually produce positive results. I

think what we have to make sure is that in every country and at an international

level, it is seen that way, that all governments actually seek this dialogue

with civil society and with enterprises, and the other actors as well, because I

think this precise dialogue can help, for instance, the process of legislation

and the legislature of every country to draft -- or to draft international

legislation and standards. And I think it's precisely generating this sense of

trust that has been mentioned a lot in this panel amongst the different actors,

which can actually enhance a stronger position, vis-a-vis those

that are

attacking privacy or using the communication for criminal actions.

>>MARC ROTENBERG: Thank you. We're actually heading toward the end of this

session, and with your permission, I'd like to propose the following. We will

take three more questions from the audience. I see many hands -- more than

three go up but we'll take three -- I'd like the opportunity to ask one more

big-picture question of the panelists, and then we will turn to our chairpersons

for concluding remarks.

So if I could see your hands again, please, and certainly if someone has not

yet had an opportunity to speak. You, sir, in the front row.

>>SULIMAN MUSTAFA: Thank you very much. My name is Suliman Mustafa. I am from

the Ministry of Telecommunication and Information, Sudan, and I am currently

leading a small team of -- Arab group of cybersecurity virtual group. I belong

to legal (inaudible) state.

My comment is that I do agree with the speaker who says that openness and

security and privacy are not versions to each other, rather they're complementary.

However, also in terms of the situation of cybersecurity, it is a worldwide

problem, okay? So my comment is that how possibly we are -- through the IGF we

can propose an idea that -- how we can -- in a national level, people have their

own laws and own technical and operational process. However, the issue is

worldwide. So how possibly we can be able to build something at a national

level, then we can have on the regional level, and again worldwide level through

IGF initiative that -- so we can be able to face the cybercrime or cyberthreats

issue.

In my opinion, the situation is really terrible. However, it is not that

fearful, because if there is research working on to create some solutions, and

if you consider those solutions already happening, ISO and ITU and E.U. and U.S., so how we can be able to put those countries who are in a low situation, however the Internet are growing over there, so the situation will become worse in those countries as well. So how possibly we can carry something that will be able to built step by step until we can be able to cover the issue of cybersecurity in general? Thank you very much.

>>MARC ROTENBERG: Thank you. So the question concerns new strategies for cybersecurity, both at the national and international level. Do we have comments from our panelists?

Well, if not, thank you for the question. We'll simply continue, maybe add a question to the queue.

Yes, in the back over here, please.

>>CRISTOS VELASCO: Good evening. My name is Cristos Velasco, Director-General of NACPEC.org and Ciberdelincuencia.org. It was mentioned at the beginning of this panel that the aspect or the issue of identity theft was going to be raised during the panel, so I would like to -- this issue should be addressed because, well, identity theft is both a consumer protection and a criminal issue under most countries' -- under most countries' legislations, so I would like to see what you think about this issue and what are the policies, the current policies, the current European policies and American policies, with regards to identity theft? Thank you.

>>MARC ROTENBERG: Yes. I want to thank you for this question on identity theft. It was recently reported in the United States that over 9 million Americans have been subject to this crime, which is about one out of every 30 Americans have expressed identity theft, so this is a serious problem and certainly welcome the insights of our panelists.

>>BRUCE SCHNEIER: I can start. I actually don't like the term "identity theft." I mean, if you think about it, your identity is the one thing about you that cannot be stolen. What this crime is, is fraud due to impersonation, right? It's not new. It's millennia old. What makes it new, what makes it different, is that it's automated and it's done remotely, and it is very profitable. And it's very international.

We seem to be doing pretty well against it. It is very common, but if laws are set up right, it's relatively easy to clean up.

The issue seems to be, is who is liable for the identity theft? Because if you think about it, if someone goes to my bank, impersonates me and steals money out of my account, I'm not involved, and if I'm liable for the loss, then there's no way for me to improve the bank's security.

So as long as we build a legal system where the entity who is responsible for the risk is liable for the risk, then security naturally improves and you see that over the decades with credit cards or with check fraud.

And when we have that, identity theft is mitigated down to reasonable levels of fraud that we accept in society. In areas where you have that mismatch, where the individual is liable for the fraud and the company is in a position to mitigate the fraud -- for example, toll fraud in Canada -- there you have serious problems which can't be fixed, because the economic incentives just aren't aligned right.

>>JOSEPH ALHADEFF: The only thing I wanted to highlight is I think if we take some lessons from other situations like spam, the concept of a legislative fix by itself I don't think is enough and I think that might be the case with identity theft also.

I think you need more of a multipronged approach and I think you need more of a

cooperate and a collaborative approach. That doesn't mean that legislation wouldn't be part of it, but I don't think you fix it completely with legislation, so I would think that we -- much like security is a concept of defense and depth, I think solving these problems is not just a legislative solution, but it will involve education, it will involve outreach, it will involve cooperation, it might involve new technologies and legislation that may well be part of the solution as well, but not, I think, by itself.

>>MARC ROTENBERG: Okay. And our last question will be from Bill Graham of the Internet Society.

>>BILL GRAHAM: Thank you, Marc. I'm actually channeling Michael Nelson, visiting professor of Internet studies at Georgetown University, who was having some problems with the remote site. He says, "I've found this panel to be a valuable and balanced discussion of a very complex set of topics, but like our moderator, I'd like more specifics.

Much of my research and writing is about cloud computing and barriers to its adoption. I'm particularly concerned about policies designed to protect privacy or intellectual property rights being mis-applied in ways that could stymie development and use of new cloud services. How can we future-proof, copyright privacy laws so users can enjoy the potential of these new services while ensuring choice and transparency and accountability?" Thanks.

>>MARC ROTENBERG: Anyone want to take this on? Well, this is interesting.

So maybe we can take one more question, then. Okay. So in the middle here, please.

>> Yeah. Let me introduce myself first. I'm (saying name). I'm working in ITIDA, the Information Technology Industry Development Agency, Egypt.

This is a question for all the panelists, actually, since Mr.

Rotenberg just

said that it's the individual choice either to choose to share his information,

and to lose his privacy, or he can choose to keep his information and with that

he will keep his privacy.

But I think this was not the reason Internet was founded for, in the first place.

I think it was founded to bring people closer to each other. So that can -- I

can use this part of trust that all the -- most of the people talked about today.

Because maybe I will -- I want to -- I want to choose to share this information

with my closest friends or family or somebody I really trust, but there will be

other parties that will be willing to share this -- that I will not -- that I'm

not willing to share this information with, but they will be seeing this information.

So let me share a very small story with you. It's about a very old guy that

was living in the U.S. for 40 years and he woke up one day and he found himself

wanting -- sorry, he found that he wanted plant some potatoes and herbs in his

garden so he sent an e-mail for his son that was studying in Paris telling him

that, "I would like to plant some potatoes but you are not around to help me and

I'm very weak to do so alone," and so his son answered him by saying, "My

father, please do not touch that ground, the garden, because I buried in it the

thing." And the second thing the FBI was all around his garden digging every

part of it, and they didn't leave any part, and then they left because they

didn't unfortunately find anything.

Then the son sent another e-mail to his father saying, "I think, father, the

ground is all digged and you can plant your potatoes that you wanted to."

So that's the end of my story, but I have another thing to say.
It was, I think -- it was all over -- it was all got over when we had this

iPhone, which is linking to our Mac computer, which has all the information about us. My name, where I'm living, where I'm staying, whether I'm staying with my friends in Cairo or in Sharm or in Luxor or whatever, and according to the Mac computer and the iPhone, all the information I have in my life is exposed.

And as Mr. Joseph just said, that we can delete the source but we cannot delete

its tail, so I really would like to hear from the panelists their opinion about whether I should be sharing my information with everybody, including other parties that I do not really want them to see whatever is happening in my life, whether I'm staying in someplace or whom I'm writing to or whatever I'm writing

to, because my -- both sisters are not living in Egypt, so if I'm going to write them an e-mail and this e-mail is going to be exposed, then I think I better

call them over the phone. Other than that, maybe the phone is -- also can be

heard. So thank you so much.

>>MARC ROTENBERG: Okay. Thank you for this comment. I'm aware that we are

running out of time and we have, in addition to our closing remarks, also some

remarks from the Secretariat, and I would very much like to ask this final

question, but given the limited amount of time we have, I'm going to ask our

panelists to be very brief, just a sentence or two, please, in response to my question.

And my question is this: Assuming you had a few minutes with your minister of

communications to make a specific recommendation about the future of the

Internet, something you would very much like to see your country do that you

think should be a top priority, what concretely, what specifically would you recommend to your minister be done? And I'm going to start with Joe.

>>JOSEPH ALHADEFF: I guess the concept would be a three-fold thing and it's a short -- consultation --

>>MARC ROTENBERG: To do that in a sentence it could only be with semicolons.

>>JOSEPH ALHADEFF: Okay. I won't elaborate on the three concepts but it's consultation, narrow tailoring, and observe for unintended consequences.

>>MARC ROTENBERG: Okay. Fair enough. Ms. Hoepers.

>>CRISTINE HOEPERS: Well, actually in Brazil it wouldn't be the Minister of

Communication it would be the Internet steering committee and they are actually

in the room and I talk to them a lot but I always say to them, for me, the first

thing, the most important thing, is education.

>>MARC ROTENBERG: Education. Thank you. Ms. Malhotra.

>>NAMITA MALHOTRA: Is it working? Yeah. I think the question would be some

kind of illusion because I would reiterate what my presentation said, that it

depends on who you are, where you are, where you're located, whether or not this

conversation is even possible. So I would just say that. I don't think it will happen.

>>MARC ROTENBERG: You don't think it would happen, okay. Well... Bruce Schneier.

>>BRUCE SCHNEIER: I think you should clean your own house, improve your own

security. I think you should use your buying power to convince vendors to

improve the security of their products, and I think you should fund research

broadly and widely.

>>MARC ROTENBERG: Very good. Mr. Seger.

>>ALEXANDER SEGER: I would focus on something that I can actually support and

where I can help deliver and, therefore, I would say I would like -- I would

recommend to implement the Convention on Cybercrime, to implement

data

protection legislation along a treaty that is already available at the Council of Europe, and to, in the country, build the capacity for that and, moreover, promote globally that these treaties and these standards are implemented.

>>MARC ROTENBERG: Thank you. Mr. La Rue?

>>FRANK LA RUE: Two things. I would first try to convene a mechanism of consultation that draws all sectors in and try to build a consensus and a position that will help draft a human rights-based policy on communication and on criminal action and prosecution of that, and specifically the protection of rights including privacy.

And the second thing, very concrete, is I would suggest to my ministers to establish a fund be to subsidize the access of communication of all those sectors that have not had access to it or have not had any training or education on it.

>>MARC ROTENBERG: Very good. Thank you. And now, I think the Secretariat has brief remarks. Yes? Markus? Can we get a microphone here, please?

>>MARKUS KUMMER: Thank you. Just a few words about the change of program on Wednesday. As I noticed, there was some confusion. We will change the program due to the appearance of the first lady of Egypt at our meeting, so all workshops on Wednesday morning will now start at 8:00, and not as scheduled in

the printed program, but as it is on our program on the Web site. All workshops will start at 8:00, and the buses will be rescheduled accordingly.

I think they will leave from the hotels at 7:00 instead of at 8:00. It's just they will be in time. As well, there will be notices up at the hotels.

At 9:30, all workshops will end, and then participants will have time to come into the main session hall. The doors here will be closed at

quarter to 10:00

for security reasons and a special honorary session will start at 10:00. We'll go through until 11:15, and at 11:30, the normal program will resume.

We will break for lunch at 1:00. We will resume again at 1430.

That means that the main session on the stock taking will be broken up in two parts, the first part in the morning and the second part in the afternoon. And

the last substantive session on emerging issues will start at 4:00. It will be

reduced slightly. It will be two hours and not two and a half hours, so it will

be between 4:00 and 6:00. And the closing session will then be at 6:00, and we

will end the program at 6:30.

We will not have much margins because of the interpreters who will not be able

to work for longer than that.

So we will have a very tight program on Wednesday, but I'm sure it will work

out all right.

And the second announcement was, I would like to announcement the launch of the

Global Information Society Watch 2009 by the Association for Progressive

Communications. It will take place at 6:30 in the lobby next to the restaurant

here in the conference center.

Once again, the book launch Global Information Society Watch at 6:30 in the

lobby next to the restaurant.

Thank you.

>>MARC ROTENBERG: Thank you.

And now to conclude our afternoon plenary session, Dr. Hashem and Minister

Matic.

>>SHERIF HASHEM: Well, I personally enjoyed the discussions, the thoughts

that were shared by the panelists and the audience, the participation.

I would like to highlight, in conclusion, the importance of trust. When we

talk about security, privacy, openness, it's about the trust. The Internet --

People use the Internet and they trust that this is a viable media for them to exchange their views, to have their dreams, to realize these dreams, and through their work, cultural exchange, to understand about other cultures. It's very important that this trust is really not undermined by criminal activities or other threats. So education and openness are key to achieve such a trust. Trust is a result, not a concept that we start off with. And to reach education, we have to revise our messages, the awareness. Most people would agree that security is important, that privacy is important. But the problem is once this is agreed upon, the translation of how this translates on how we do business, how we share our private information to the extent that it doesn't really undermine our security. When we deal with security, when you talk about really security within even a business environment, a CEO would be convinced that security is important. But how much budget is allocated there? It's critical. Especially, security experts, and I have a few of my colleagues working in this area, it is sometimes frustrating. You are asking for a budget and the best results that you show is that nothing happens. You are able to really avoid threats, but how you materialize this is very important. So again, the concept of education, involving all stakeholders in the community. Children, teachers, judges, prosecutors, law enforcement officers, lawyers, technology providers, decision-makers within government, private sector, social, society organizations, to make sure that everybody understands the message. The message is clear, and the game, or, really, the challenge is there. The trust is what we are after. We would like to achieve that result with really a coherent framework, cooperative framework that

involves all

stakeholders so that people are not marginalized. They feel that they are part

of the activities, and it is really part, and it is reflecting on their lives

the way they would like to see it.

With this, I would like to conclude, and I hope that the message was clear to

the audience. And I really look forward to the interaction beyond this session.

>>H.E. MS. JASNA MATIC: I don't think there's too much to say in conclusion.

I think one thing is clear, however; that there's clear need for continuation of

the Internet Governance Forum discussing on this topic, also. And it's clear

that this needs to be a multistakeholder, collaborative process with roles and

responsibilities for all of us. And we all need to keep track of technology

with the social dynamics, which is evolving on a daily basis. The regulators,

the legislators, the corporations, the civil society, we all need to follow

what's going on in order to be able to cope with it, and to be able to use this

wonder of Internet and not let the bad things prevail.

>>MARC ROTENBERG: Well, thank you for a wonderful panel discussion. May I

ask you all to give a hand to our fine panelists.

[Applause]