RAW FILE
October 24, 2016.
1430.
World Telecommunication Standardization Assembly primary session.

***.

October 24, 2016.

1430.

ITU.

World Telecommunication Standardization Assembly.

Primary session.

October 24, 2016.

1430.

ITU.

World Telecommunication Standardization Assembly.

Primary session.

October 24, 2016.

1430.

ITU.

World Telecommunication Standardization Assembly.

Global Standards Symposium

Primary session.

>> Good morning, ladies and gentlemen. Welcome to this Global Standards Symposium. There is free seating today. You can sit wherever you would like to sit today. The nameplates are installed for tomorrow's WTSA, so there is free seating today.

You can pick whichever seat you would like to pick..

Good morning, ladies and gentlemen. Welcome to the Global Standards Symposium. You can sit wherever you would like to sit today. The nameplates are installed for tomorrow's WTSA, so there is free seating today. You can pick whichever seat you would like to pick.

Good morning, ladies and gentlemen. Welcome to the Global Standards Symposium. You can sit wherever you would like to sit today. The nameplates are installed for tomorrow's WTSA. So there is free seating today. You can pick whichever seat you would like to pick.

Good morning, ladies and gentlemen. Welcome to the Global Standards Symposium. You can sit wherever you would like to sit today. The nameplates are installed for tomorrow's WTSA. So there is free seating today. You can pick whichever seat you would like to pick.

Ladies and gentlemen, please be seated.

Ladies and gentlemen, welcome to the GSS 16. Please be seated. We will be starting in a minute. Thank you very much.

Ladies and gentlemen, please have your seats. We are starting the GSS 16 Global Standards Symposium. The room will have interpretation in the six languages. Please use your headset. We will turn off the loudspeaker, because we will be running into the six languages. So we are just going to use the loudspeaker for now for the beginning, just for this announcement. Then please use your headset, and as you know, the channels of the 6 languages will be available in for interpretation.

English is on channel 1.

You will also find a microphone on your table, where you can request the floor. It is an automatic system. You press the button once. It will be flashing red. Once the Chairman recognizes you, it will be solid red and you can speak. Once you are done, you don't have to press it again. It will turn off automatically.

Joining us on the podium will be His Excellency, Minister Mohamed Anouar Maarouf, Minister of Communication Technologies and Digital Economy, Republic of Tunisia. Mr. Houlin Zhao,

Secretary-General of ITU, and His Excellency, Habib Secretary of State for digital economy, and His Excellency, Dr. Chaesub Lee, TSB director.

Ladies and gentlemen, it's an honor and privilege to invite His Excellency Mohamed Anouar Maarouf, Minister of Communication Technologies and digital economy, Republic of Tunisia to give the welcoming remarks.

>> MOHAMED ANOUAR MAAROUF: Merciful god for the compassionate, Mr. Chaesub Lee, Mr. Houlin Zhao, Secretary-General, Secretary of State for the digital economy, ladies and gentlemen, guests of Tunisia, heads of enterprises, experts, executives, professionals, in the ICT sector, welcome to Tunisia.

Today we are pleased and proud to welcome you here. Your presence here within the framework of a very signal international event in the Telecom sector leads us to be particularly proud. The subject that you will be dealing with here are all vital interest.

They reflect and they take into consideration the centers of interest of all of us working in this sector, and well beyond. It goes without saying that many of you present here this morning are visiting Tunisia for the first time.

To those, we would wish an especially warm welcome.

And it is my pleasure to express to you the appreciation of the government and people of Tunisia to you. We are proud to have you here with us, and we are very proud to see that your choice has been that of Tunisia, as a venue for this meeting.

We are also proud to see the number of participants. We are nearly 1,000 here coming from over 100 countries. For the very first time in the history of the WTSA, and for the very first time in the history of Tunisia, so we would like to express our appreciation for the trust you have accorded Tunisia, and we hope that we will not disappoint you.

Please be aware that you can count on us at any and all times, during your stay in Tunisia, for the WTSA.

I'm not going to be too long. But let me just say that the issues that you will be tackling will all be of crucial interest to the ICT. Trust is the key word for this meeting, and confidence. The world is entering a period of huge innovation with many different actors, and all of these efforts will only meet with success if we have a fundamental element as a part of it, and that is trust.

The superior Council of the magistrature in Tunisia has made a historical decision concerning the bolstering

of Democratic institutions in this country, Tunisia indeed wishes to also have this play a major role in the Telecoms field.

Now, I know that you have a very busy agenda today, and over the course of the coming two weeks. During this WTSA.

But I would like to take this opportunity to remind you that you should take some leisure time, to visit Hammamet, which boasts one of the best beaches in Tunisia. In fact, Hammamet beach is one of the 20 top ranked in the world. So in addition to your intense work here, please be our guests, do enjoy some leisure time on the beaches, visit our historical monuments. We have prepared a programme of visits, and I invite you to take full benefit of that.

We have, as you know, taken all of the necessary precautions for your safety and security, and to be at your service, so that your stay here will take place in the best possible conditions. We will remain at your disposal throughout the meeting, up until the time you will be leaving.

Now without any further ado let me again reiterate our welcome to you and our appreciation and I wish you full success in the WTSA. Again, thank you very much

for having chosen Tunisia as host of the meeting.

(applause).

>> Thank you very much, Mr. Minister. Ladies and gentlemen, excellency, it is now my honor to give the floor to Secretary-General of the ITU Houlin Zhao who will be proposing a Chair for this WTSA.

>> HOULIN ZHAO: Excellencies, dear delegates, dear participants, good morning. Minister, we thank you very much for your warm welcome. This place I'm very familiar with. I did not come for the first time. I'm familiar with because of recent years, particularly after WSIS second phase, during Tunis in November 2005, Tunisia organized ICT forum, was here. So at least I came here for that ICT for development forum for at least three times. So I'm very familiar with this place. Of course, I was also familiar with the top beaches in the world. And this beach is one of them. But I never got a chance to swim in that. But I hope this time, I can find some time to test the water, and hope you will enjoy it.

Ladies and gentlemen, for this GSS we need a Chairman. It is my great pleasure to propose His Excellency the former Minister, my friend, Mr. Mongi Marzoug to be our Chairman of the GSS. I seek your approval.

(applause).

>> HOULIN ZHAO: Great. I think we have a Chairman now. (chuckles).

In fact, it was him, Mr. Mongi who invited me to join ICT for development forum, November, 2013. That was my last time to come to this building.

>> Thank you very much, Secretary-General. We now give the floor to the Chair of the GSS 16, Mr. Mongi Marzoug.

>> MONGI MARZOUG: In the name of god, the been efficient, merciful, peace be with you all.

I'd like to thank you all for your confidence and trust in me to Chair the Global Standards Symposium in its third session.

I'm greatly honored and I wish us all success in our joint efforts, so that we effectively can contribute to the success of WTSA on issues of crucial importance to all of us in the cyberspace, the ICT space. These relate to security, privacy and the building of trust.

Mr. Houlin Zhao, welcome in Tunisia, ITU Secretary-General. Mr. Chaesub Lee, Director of TC B at ITU, Excellencies, ministers, ladies and gentlemen, head of delegations from various countries and representatives of international and regional agencies, ladies and gentlemen, CEOs of firms and economic,

financial and technical agencies operating in the field of ICT, honorable guests of Tunisia, ladies and gentlemen, it is a great pleasure for me and an honor to welcome you all to GSS 16, and I'd like to particularly thank ITU for organizing the symposium and holding WTSA in Tunisia.

We all know that these proceedings will shape ITU standardization work for the 2020 time frame. I would like also to thank all national institutions and international firms that sponsored this event, and all those who have contributed towards its preparation and success.

It's a pleasure to welcome all the leading personalities attending here, and representatives of Tunisian companies and international companies operating in the digital field, as well as academia, researchers, civil society representatives and media professionals.

I'd like to seize this opportunity to remind of Tunisia's pioneer role in building the information society, having hosted in 2005 the WSIS in its second phase.

I'd like also to thank Mr. Bilel Jamoussi and the ministers for the efforts they have invested in

organizing this meeting, this symposium in Tunisia. Honorable guests, ladies and gentlemen, cyberspace or Internet space represents in terms of importance the second largest space for humanity, second only to the natural space, according to the latest ITU estimates, there will be around 3.5 billion persons connected to the Internet by end 2016.

In view of the rapid and large scale development of ICTs, the world has experienced an unprecedented quantum leap in all aspects of social, economic and political life. All nations now can avail themselves of a great sustainable development tool and improve services such as education, health and transport. It is also a tool that helps have better control over the resources and assets that manage them, ensure environment protection and advance government and corporate services, including eServices. We also expect a great deal from this momentum towards achieving the U.N. SDGs for 2030, all global fora, WSIS, NETMundial, IGF and others have emphasized that a proper use of this space made possible by ICTs requires that it should be open, secure, safe and trusted.

It also requires that all the human rights on-line and off-line should be upheld, and I would like to mention

out of these, freedom of speech, and the right to access and protection of personal data, and increasing trust in the use of digital technology is the best guarantor of its dissemination and its developments as it contributes effectively in development.

Now the U.N. assembly resolution article 10 in introduction states the following: Building confidence in security in the use of ICT for sustainable development should also be a priority, especially giving growing challenges including the abuse of such technology for harmful activities, from harassment, crime, terrorism. In the part dedicated to building confidence in ICTs, article 48, the text goes as follows.

We affirm that strengthening confidence in security in the use of ICTs for the development of information societies and the success of such technologies is a driver for economic and social innovation. In article 49, we read the following: The U.N. assembly welcomes, we welcome the significant efforts by governments, the private sector, civil societies, the technical community and academia to build confidence in the use of ICTs, etcetera.

Our symposium today for which I wish full success to the joint efforts of all addresses the importance

of the role played by standardization in building a secure and trusted cyberspace, and preserves privacy, and this from three standpoints: Government, regulatory bodies, and industrialists and standardization institutions. After this opening session there will be three sessions that will analyze issues of security, privacy and trust. We of course hope that there will be ample discussion of these among the users of the Internet, civil society, academia, experts, specialists and all this will go into a report that will include the outputs and recommendations in the last session. Honorable guests, ladies and gentlemen, we hope that this will be beneficial to all of us, especially that this deals with Cybersecurity, privacy and the building of trust in ICTs, and that this will issue effective and practical outputs and recommendations to be of use for WTSA, for the achievement of inclusive sustainable and fair development. I'd like to thank you all for your kind attendance and peace be with you.

(applause).

>> Thank you very much, Chairman. We now give the floor to the Secretary-General.

>> Mr. Chairman, your Excellency, Minister of Communication Technologies and digital economy of

Tunisia, honorable Mr. Habib Tababi Secretary of State, Mr. Lee. Excellencies, dear colleagues and participants, good morning.

Welcome to this third Global Standards Symposium, GSS 16. Let me begin by thanking our host, Tunisia, for its support to the work of ITU, and of course for its high hospitality shown to us. I'd like to just take this good case to express my personal appreciation for our host. As I mentioned to you, last time I was here, when Tunisia organized ICT for development forum I was invited by the former Minister my dear friend Mongi Marzoug, and today I see him still there.

Last night, I arrived, I was received by our Minister, Dr. Mohammed, I see the continuation of the friendship extended to us.

But more importantly, I see the former Minister and the Minister side by side at the podium, which is their very proud continuation of their ICT policy in Tunisia.

So in such wonderful environment, really I'm very pleased to come back to Hammamet.

ITU is very appreciative to your hospitality.

GSS offers an international platform to debate standardization policy. This event brings together

leaders in the public and private sector to discuss how technical standardization should respond the evolving priorities of the ICT sector. Of course, this is the third one. The first one was held 2008 in Johannesburg, and the second one was held in Dubai, 2012. For those two, I was not there, because I was Deputy Secretary-General. I have to stay at home to take care of housekeeping businesses, where Secretary-General traveled, so this time it's my duty to come to join this, and then the current Deputy Secretary-General Malcolm Johnson who managed the first and second GSS, and he has to stay in Geneva to take care of housekeeping business there. He asked me to convey his personal greetings to all of you.

The first one in Johannesburg, we are talking about developing standardization capabilities. We talked about climate change. We talked about accessibility for people with disabilities. Then the second one, in Dubai, we talked about ICT-based convergence. We talked about ICT support, vertical sectors such as healthcare, energy, and transport. The topics discussed by GSS provide a good indication of the ICT industry's priorities, over the previous years.

We see evidence of this in ITU's work. These topics

have all become essential to the work programme of ITU standardization. ICTs are helping all industries to innovate. New ITU standards are supporting medical bridge eHealth devices, smart energy grids and connected cars. Our productive collaboration with the vertical sectors has led to the emergence of a strong business case for companies in other sectors to join the ITU membership. This Friday, I'm going to room to meet with my U.N. colleague, Secretary-General, we are going to talk about cooperation between two organisations to promote ICT for agriculture. I hope in the future we will have agriculture experts to join us as well.

ICTs are also helping the public sector to innovate. Policymakers worldwide are promoting the development of a smart sustainable cities. These cities will employ a rich diversity of ICTs to increase the efficiency and sustainability of city processes.

The smart use of data will increase our understanding of whole complex city ecosystem, be helping us to identify where innovation could lead to great sustainability.

ICTs are central to visions of our future as a society. Of course, information society. Here, we see the importance of the seed of this symposium, a true ICT

environment will give users and business the confidence to use ICTs to their full potential.

New capabilities in data collection and analysis are opening up new frontier in sustainable development.

Questions surrounding security, privacy and trust, are relevant to all interests that hold a stake in the future of ICT.

For over 150 years, ITU has provided a neutral platform, global platform, to brook consensus and policy and technical questions crucial to the development of the global ICT ecosystem.

We are given life by a diverse membership, representing governments, industries and academia. I'm very proud that ITU enjoys the unique organisations in the world, in the standardization development field, that we are the only one among many others, together with many others, and we are the only one where we have governments as our funding and members. As far as industry is concerned, I'm very pleased to see that in this room, we not only have those traditional classic ICT companies, but we also have new players, such as Google, Facebook, Alibaba and the others. Of course, academia join us since 2011. ITU is well placed to provide a neutral platform to build a common global understanding

of the ingredients to security, privacy and trust.

This is possible where approach discussions from the perspectives of policy, business and standardization.

This emerging disciplinary approach is essential and inclusive. It is becoming increasingly difficult to isolate technical issues from policy issues. Therefore, we have to find ways to understand the market need and stakeholders' need to develop new technologies to satisfy them. This symposium will contribute to improve the communications among policymakers, industry players, and standard bodies.

We will learn more about issues as work help us to find new ways of working together. ITU standardization plays an important role in fulfilling ITU's mandate to build confidence and security in the use of ICTs. This symposium will host an exchange of views that will offer valuable guidance to the technical standardization community in its work to establish a trusted basis for ICT growth and innovation.

I would like to conclude by thanking all of our speakers, moderators and participants for their contribution to this symposium. Of course, I would also like to thank my friend, the Chairman of this GSS for

his own contributions and support. Open symposium such as GSS complement ITU's decision-making meetings, by airing the views of as many stakeholders as possible.

The conclusion of GSS are certain to provide valuable input to our WTSA 2016. I'd like to thank you for your attention, and wish you a most informative symposium. Enjoy yourselves. Thank you.

(applause).

>> Thank you very much, Secretary-General. Now I'd like to give the floor to Dr. Chaesub Lee, TSB Director.

>> CHAESUB LEE: Excellency, Minister, distinguished colleagues, ladies and gentlemen, it's a great pleasure to welcome you to this third Global Standards Symposium. I'd like my thanks to our host Tunisia. I thank you for your generous hospitality, and I'm looking forward to an enjoyable stay here in Hammamet.

This is my second visit, but I didn't still have yet to enjoy this beautiful beach here. So with you during this two weeks, we try to find out how we can enjoy this beautiful City of Hammamet.

Dear colleagues, ITU has a mandate to build confidence and security in the use of ICTs. We provide a neutral platform for stakeholders, to collaborate in the interests of achieving this goal. The importance

of this work is growing. As we approach year 2020, we will be working to enable, ICTs will soon support nearly every aspect of business and daily life.

The post 2020 ICT environment will provide more ubiquitous, reliable, and operable communications, and at the high end of 5G applications, ICTs will support remote medical surgery, industrial robots, autonomous vehicles and much more.

IoT technologies and applications are becoming integral to business operations and the public services, cyber systems will soon host billions of connectivity things and objects.

We are building smart sustainable communities, cities, integrating ICTs in city systems to improve efficience and support sustainable organisation.

We are connecting everything. We expect that our hyperconnected world will be a safer, cleaner, happier place to live.

However, it is clear that visions of the social and economic benefits to be enacted by emerging ICTs have a degree of trust in the information society that we have yet to achieve.

We are building connected energy, transport and water networks. ICTs are enabling the interconnection

of all types of objects, from vehicles and streetlights to the appliances in our homes.

This has unprecedented implications of data security, reliability of critical infrastructure, and the privacy and safety of the world's citizens.

Here we see the importance of ITU's work to support the development of a trusted ICT environment. We have released a technical report outlining the fundamentals of trusted ICT environment, and the future ITU standards will define the technical mechanisms to realize this environment.

Secretary-General Mr. Houlin Zhao, our increasing capabilities in data collection and analysis have opened up new frontiers in sustainable development.

It is important that technical standards have to prevent the emergence of data silos in different sectors of our economies.

Our shared data ecosystems will help us to use data driven insight to tackle the greatest challenges of the 21st century.

Experts, participating in ITU standardization, are working to support the development of this integrated data ecosystem. At the same time, the technical work aimed to protect fundamental rights to privacy, using

privacy by design principles.

This symposium will offer valuable guidance to ITU standardization how it should go about achieving these aims.

Say that I wish you a most enjoyable stay here and most good success in this symposium. Thank you very much.

(applause).

>> Thank you very much, Dr. Lee. Ladies and gentlemen, Excellencies, this concludes our opening session for GSS 16. We will go directly to session 2, which will be on regulatory principles for security, privacy and trust. Please help me -- photo? Yes. Actually, I was reminded there is a photo first. So we will have the photo on the podium with the speakers. I'd like to invite the GSS speakers to come up to the podium to take a photo with the Excellencies. (pause).

Ladies and gentlemen, please be seated. We will be starting session 2 now.

>> Thank you. My name is Bilel Jamoussi, it is a pleasure to moderate session 2 for today. Session 2 is on regulatory principles for security, privacy and trust. The idea of this session is really to get a view into the current regulatory frameworks, globally, and from those principles and frameworks to then lead into the

programme of GSS and see how the private sector is working to address some of those challenges. And then to conclude with the standards development organisations in the last session of the day, and see how the standards development organisations are working and collaborating and providing a platform to develop the technical standards to address those regulatory challenges or needs.

We would like to first start by inviting Mr. John Edwards, the privacy commissioner of New Zealand, as well as the Chair of the executive committee for the international conference of data protection and privacy commissioners.

He will be our keynote speaker. His biography is on-line on the programme. I'd like now to invite Mr. Edwards to give his keynote.

>> JOHN EDWARDS: Thank you, Doctor. Excellencies, Mr. Chairman, President, it's my great pleasure to be here. I'm grateful to the ITU for the invitation to address you and to introduce you to the international conference of data protection and privacy commissioners, which held its 38th annual conference in Marrakesh last week.

For many years I practiced law in the field of technology and privacy, the term convergence was in vogue.

I now can't even remember what was going to converge telephony and computing? Broadcasting and Internet? It was one of those terms that expanded to meet any number of needs. Convergence always seemed to be just around the corner, and whatever it was, we don't seem to hear much about it anymore. Maybe that indicates that it's been achieved.

There seems to be another convergence occurring, the gradual but accelerating consensus among previously disparate organisations, that privacy is becoming one of the defining issues of our age.

The United Nations General Assembly during its 68th session in 2013 adopted a resolution titled, the right to privacy in the digital age, calling on all U.N. member states to respect and protect the right to privacy including in the context of digital communication.

The international technology and market research company Foresters declared that 20115 would be the -- 2015 would be the year privacy and security would be competitive differentiators. We saw that happen, and for the trend to continue into 2016, we have seen Apple, Facebook and Microsoft in the courts to stand up for customers' rights to privacy, we have seen Google and Facebook and many others subject to high profile

regulatory attention of European data protection regulators.

In May this year, the World Bank issued a world development report entitled, digital dividends, which highlighted among other things the need for consistent, reliable regulation for data protection as a key factor in reducing inefficiencies and promoting consumer confidence in the on-line world.

In June this year, at the OECD ministerial on the digital economy in Cancun, participating ministers declared the importance of building and strengthening trust in order to maximize the benefits of the digital economy.

The participating OECD ministers recognized that trust, privacy and transparency are essential elements of civic and digital engagement.

Ministers agreed that they would, this is a quote from the declaration, "develop privacy and data protection strategies at the highest level of government that incorporate a whole of society perspective, while providing the flexibility needed to take advantage of digital technologies for the benefit of all, and support the development of international arrangements that promote effective privacy and data protection across

jurisdictions including through interoperability among frameworks."

The OECD earlier declared the importance of a multistakeholder approach t ITU it seems to me is very much a multistakeholder organisation, and it has clearly recognized the importance of privacy and security to its membership by organizing this conference, and in so doing, converges with the work of the World Bank, the E OCD and -- OECD and international conference of data protection and privacy commissioners which I'm representing here today.

In my brief comments, I'd like to give you a bit of the history of my organisation, mention some of the work that me and member authorities are undertaking in areas of common interest to your membership and outline areas of possible future collaboration.

The first conference of privacy commissioners was held in 1979. There were no formal membership criteria, but invitations were extended only to data protection authorities with a mandate of a public sector organisations. In 2001, the conference first adopted membership criteria. 54 authorities formed a foundation membership and by 2010, the conference had grown to 89. The coverage grew to include agencies with a solely

private sector mandate, including the Korean Internet security agency, KISA, in 2004 and the U.S. Federal Trade Commission in 2010.

The conference rules and procedures adopted in 2010 set out five substantive membership criteria, to be a member a entity must be a public entity created by a appropriate legal instrument, must have the supervision of the implementation of data protection or privacy law as one of its principal regulatory functions t law under which it operates is compatible with the principal international data protection or privacy instruments and appropriate range of legal powers to perform its functions and appropriate autonomy and independence.

In the 14 years since 2002, when membership was first established, the conference has grown from 54 to 115 members. In other words it has more than doubled in size, reflecting a expansion in data protection laws around the world. While there may be encouraging for anyone that values the idea of more universal data protection law, the growth should be seen in perspective. Note for example only about one-third of the 193 U.N. member states are represented in the conference.

Only three of the 20 most populace countries have authorities that are members of the conference. Some

two-thirds of the conference membership is from one region. Our conference from time to time convenes working groups to undertake research or develop policy on particular issues. One working group of particular relevance to the ITU is the international working group on data protection and telecommunications, which is known as the Berlin group.

The Berlin group has met twice a year since the early 1980s, and consists of 55 participants representing 36 delegations. Last week in Marrakesh the Berlin group reported back on its activities in the last year, including issuing working papers on location tracking from communications of mobile devices, intelligent video analytics, and an update on privacy and security issues in Internet telephony, VOIP and related communication technologies.

In this last paper, available on the group's website, the group calls upon legislators and regulators to ensure that the provisions for telecommunications secrecy as foreseen in many national constitutions and regional and global regulatory instruments also fully cover VOIP and other multi media communication services.

In addition, the paper contains recommendations on privacy and security for VOIP providers, software

developers, hardware manufacturers, and for users. The group has also led an ongoing discussion about the use of biometrics in electronic authentication. You will appreciate the significance of this issue, given that you can change your password or cell phone number but it is not so easy to change your voiceprint or retina.

One of the reasons we are so focused on privacy, particularly in telecommunications at the moment, is because of the disclosures of the former NSA contractor Edward Snowden. I don't need to remind you of the details, but the Snowden revelations sent shock waves through the privacy telecommunications and IT worlds.

The allegations that intelligence agencies routinely received access to vast amounts of data both in transmission or on the servers of on-line platforms ignited conversations and debates as well as inquiries, court cases and law reform in many countries around the world.

The allegations had potential to undermine what the OECD has identified as that necessary precondition for the effective operation of the digital economy, trust. The responses were immediate and wide ranging. The U.N. moved that same year to appoint a Special Rapporteur on the right to privacy. He is today making his report

to the General Assembly.

I add without comment that our conference first passed a declaration calling on the United Nations to prepare a legal binding instrument which clearly sets out the rights to data protection and privacy as enforceable human rights in 2005 in Switzerland. We are yet to see such a instrument but perhaps when the Special Rapporteur completes his mandate the U.N. will have a sound basis to do that work.

If the Snowden revelations eroded trust so too does the seemingly endless parade of leaks and breaches criminal and state sponsored which compromise networks, databases and consumer and business confidence in the digital infrastructure. The question is then, for the many agencies and interest groups converged on this problem, how to build and maintain that trust.

The ICD PP C has undertaken some work in this area, but it will take the kind of multistakeholder approach sought by the OECD and represented by the ITU to ensure the comprehensive and coherent response to these issues as the digital world continues to expand and more and more economies begin to rightfully demand their digital dividends.

Here are some ideas for shoring up that confidence

and trust by applying privacy principles that represent regulatory norms around the world, and perhaps developing standards in the communications sector. First, promote and deploy privacy by design, privacy impact assessments and privacy enhancing technologies. There is no trade-off to be made between innovation, enterprise and privacy. Good privacy and security practices when designed into new technologies become a selling point and improve the whole network.

Ensure access to networks, systems, content, communications and metadata by agents of the state is undertaken only in accordance with lawful authorities and where that access is necessary and proportionate.

Privacy is a fundamental human right but like many other rights, it is not absolute. Just as I cannot exercise my right to freedom of expression in this room to shout, fire! Nor can I exercise my right to privacy to prevent the detection of a trade in child pornography. Access to communications by law enforcement, security or intelligence agencies should be according to consistent legal standards regardless of the jurisdiction.

We could promote transparency in relation to access or use of personal data for purposes other than those

for which the data is collected or to which the data subject has consented.

What shocked many about the Snowden allegations was that platforms, many use on-line, many of us use on-line on a daily basis were allegedly freely available to agencies for intelligence purposes. Several of the most prominent on-line practices responded with regular transparency reports, in which they revealed to the customers and the world the nature and extent of official calls on their customer data.

The Berlin group and ICD PP C in 2015 passed resolutions supporting and promoting transparency reporting from telecommunications and ICT platforms among others.

We could develop and promote appropriate standards and safeguards for the de-identification of personal data and for the prevention of re-identification of individuals from de-identified data sets.

Industry and government alike are clamoring to reap the benefits of so called big data. The ability of data scientists to derive public benefits from analyzing large data sets is undeniable. Telecommunications companies have data with which much good can be done. With location data, for example, NGOs and aid agencies can track the

movements of refugees after political upheaval or natural disaster or trace the spread of disease. The U.N. global pulse which is established under the office of the Secretary-General has developed a set of privacy principles to try and facilitate this kind of work.

To get the social benefit of such data, it is not necessary to identify individual mobile phone users, and to do so would in many cases breach privacy principles but how do we know that a measure to de-identify a data set will be effective. Data protection authorities and privacy commissioners heard at our Internet of Things session in 2014 that researchers have proven the ease with which individuals could be extracted from a supposedly de-identified data set. They found that if they have a data set including the location details of 1.5 million mobile phone users over a year, and they knew where one individual had been only four times in that year, they could extract that individual's full location history from that 1.5 million data set within 85 percent accuracy. Sometimes de-identified does not mean de-identified.

We can ensure citizens and consumers have transparency on the basis of which automated decisions affecting them have been made. We heard last week that

even as a still quite undeveloped and not widely understood the concept of algorithmic transparency is facing considerable challenges in the light of artificial intelligence, machine learning, and unpredictability by design.

Data affordability is a area requiring further work in standards. Just as affordability has proved crucial in improving competition in the mobile phone industry so is a important concept in promoting consumer rights and facilitating the ease of access to and exit from telecommunications on-line and other services.

Data port ability is part of the European general data protection regulation due to come into effect in 2018, and will be needed to be provided for beyond Europe.

In closing I want to say I hope that my organisation and the ITU will have further opportunities for our organisations to work together and I look forward to a continued exchange of speakers for our respective conferences. I would welcome, a proposal for the ITU to attend our 39th conference in Hong Kong next year in some capacity either as observer or host of a side event.

I'm sure members of the ICD, PPC would welcome the opportunity to join ITU Study Groups or to attend the

regional meetings which make such a contribution to your work.

One thing that has become very clear to our conference is the data protection authorities and privacy commissioners cannot resolve the challenges presented by the new technologies on our own. We must work with industry, government, NGOs, academia, and organisations such as yours, to ensure that all can participate safely in the digital economy.

I am very grateful for the opportunity to address you. I look forward to participating in the ongoing conversation.

Thank you very much.

(applause).

>> BILEL JAMOUSSI: Thank you very much, Mr. Edwards, for a comprehensive perspective, global perspective on data privacy and protection issues. And the pointing out some of the areas that require further technology in standardization development, and you mentioned privacy by design and privacy enhancing technologies, and various standards activities that could be developed to enhance and meet some of these challenges. Thank you very much for that global perspective. I'd like now, ladies and gentlemen, to invite Mr. Victor Manuel

Martinez Vanegas, director of international policy in telecommunications institute from Mexico, to share with us his perspective.

>> VICTOR MANUEL MARTINEZ VANEGAS: Thank you for this kind invitation, it is an honor for me to be here with you, dear colleagues, ministers,
Mr. Secretary-General and all of you. For me, this is very important to be here, because maybe you know in Mexico there are new constitutional reform that create the federal telecommunications institute in 2013. My institute is in charge of the regulatory principles of the Telecoms and broadcasting services, and also is the competition authority in these sectors, and is also the body in charge of the standardization sectors. With this, let me change to the Spanish in order to be more clear in my concepts.

First, moving on with the presentation, as I was saying about constitutional reform in Mexico it very much affects Telecoms. We have a authority which is a public entity, which is independent of the government, and which has the same development objectives as the government, and of course respects all international commitments that Mexico has subscribed to.

Now, we have listened with a great deal of interest

to the distinguished previous speaker, Mr. Edwards, so first of all, let's look at the international principles that I think we have all reached agreement on and the terminology that we see here. We think this is very important for socioeconomic development of our countries and at the same time there are true risks in terms of security and privacy as well as a trust in the system.

As we have seen throughout history, and in particular following the first phase of the world information conference, we often see reference made to the importance of a trust confidence in security in ICT. The Geneva meeting, ministers of recommendations, that ITU would be a facilitator for the development goal number 5, Sustainable Development Goal number 5, also there is a global Cybersecurity agenda, the ITU, which is very important for the different measures that are flagged in it as legal measures, capacity-building, international cooperation above all, all a part of this. Also the General Assembly in the meantime set up a group of governmental experts on the developments in the field of information and telecommunications, in the context of international security.

All of these, all of these in their efforts have led to changes, especially in Mexico, which now are

reflected in our constitutional reform. Let's look at E-Trade now. Here we have a very fundamental element, there is a UNCTAD information report in 2015 which mentions frauds and different risks that can occur in eBusiness, not only does it go into some legal responses to these different kinds of illicit activities, but it gives us a series of technical measures to help strengthen security, and consumer defense in our networks.

Let me also mention the TBD agreement, with the world trade organisation, which does feel first of all with regulation on the protection of different citizens in different countries.

I should also cite the World Economic Forum, which dealt with cyber attacks which it saw as a global risk and one of the most acute ones. Now, what is important in the ITU from my point of view is this, well, work in Study Group 17, we have been very active there, and have been working for the last three years, focused on the work to be performed by this Study Group. And here I've listed some of the links that it's working on at this time, developing things like a roadmap for security standards, to try to give us a global view, and also a very specific view of the different standards that are being developed.

I think it's very important to take these into consideration on a national level. The ITU-R of 2012 also -- ITR did a great deal of work on security and robustness of networks, and we think that it's a very important that this be part of our regulation.

Now, the IEC has also been developing some standards, and working hand in hand in the case of Mexico with the Ministry of the economy.

Now in the organisation of American states, we have an organisation called CITEL which deals with, at this time is dealing with questions of security and governance. I think we were able to glean a great deal of valuable information, and this is an excellent international forum for activity in this field.

Well, I could also mention the IDB or the OECD, Mexico is a member of these organisations and participates in their activities in this field. The OECD has several different avenues of effort here, in terms of privacy and its protection. APEC has also for several years been working on the flow of information across borders, and has listed several preferred practices. We feel that with all of this, we can say that there is an entire gamut of very good international norms here, some of them very interesting. At the same time, there

is the problem of how to apply these concretely on a national level.

First in Mexico, well, international activities are very interesting to us and very important, but in Mexico we have tried to put a national twist on things. I would just cite for example in the constitution a maximum level of guarantees for access of citizens, in article 6 of the constitution we have, we established the right to privacy as a fundamental right of citizens, as well as accessing telecommunications services and all sorts of broadband.

We have also set up an organisation that I have the pleasure of working in, that deals with, well the federal telecommunications institute which is a regulatory agency, one of its main tasks is indeed protection of personal data.

So what I wanted to emphasize here was the national twist that we put on all of these. We have got two organisations on the same level, constitutional level then, that you can see up here. This again has to do with protection and greater security in ICT.

What about our national legal framework here? Here I have a list, first of all the general law of transparency and access to public government information, for federal

consumer protection law and then we have industrial property law, copyright law and a federal Telecom and broadcasting law. The last one is one that is part of our Telecom institute. There are two main points here that have to do with security and trust and privacy.

One of these is something that was tested with cooperation with the justice system. This has been very important for us, because this was done, these guidelines were drawn up to involve all of the stakeholders, consultations were held on security and justice matters, not just with the Ministry of justice but other stakeholders as well.

This has been going on for some two years since it was made official, and several topics are currently on the agenda. One of them has to do with many of the things we are going to be dealing with on our agenda, such as seeing standards as a real possibility to immediately stop any kind of stolen equipment or material, and prevent trafficking say in portables.

Also, any kind of fraud that takes place, falsify equipment, the withdrawal of youth committing crime so with that we hope that we will be able to further improve cooperation in this respect.

There are a few other regulations.

One has to do with organizing the network. We are always aiming at protection of data that these networks contain. Well, anyway, that is the Mexican perspective on this. Thank you very much.

(applause).

>> BILEL JAMOUSSI: Thank you very much, Victor. Thank you very much for sharing also a pretty broad and global perspective and not only from Mexico but also what is happening around the world on this topic. Thank you for that.

Ladies and gentlemen, it's my pleasure now to welcome Mr. Ilias Chantzos, Senior Director, Government Affairs, EMEA, with Symantec. He also has been working closely with the regulators on this topic. He will share with us his view as a private sector company interfacing with the regulators.

>> ILIAS CHANTZOS: Thank you, Chairman. I'd like to thank you the organizers for giving me the opportunity to be here with you today.

Ladies and gentlemen, discussing about security and privacy is always a complicated topic, and it's even more so when you are looking at it from the perspective of a company whose mission is to provide technologies, to provide capabilities that will ensure security and

privacy.

We have heard many of the previous speakers mentioning about why this is important, or why this will drive future discussions. I'd like us to ask ourselves, perhaps an even more basic question: Why has it become important? What has fundamentally changed? Looking at it from the point of view of, because you know what, when I started back in 2000 on Cybersecurity issues, Cybersecurity privacy was a good to have, was something extra, was something positive, but it was not necessarily the number one priority. You know what? Right now, Cybersecurity, privacy have been catapulted, have been massively pushed to the fore of this discussion. So much, that we have a illustrious panel and such a debate within the ITU.

If I take a step back, first of all, the use of technologies, the use of technologies that we do right now has fundamentally changed, because we are for the first time let's say at the moment whereby we see a massive technological shift towards the use of data. If you see the way we consume technology right now, and the way we expect that we will consume technology, either because of the Internet of Things or because of cloud computing or because of mobility or because of big data and

artificial intelligence, the reality is that they are expected use of technology will radically shift from the existing technological paradigm.

And linked to that is the realization that a cyber incident attacks, accidents, pick, you know, even mistakes from well intended users, go beyond a nuisance. Do you remember times that we had computer viruses that, you know, what would basically make our computer go slower or delete perhaps a file or two that we have saved but otherwise not do any significant damage? We have gone now to the complete other extreme because we are faced now with situations whereby cyber attacks target our critical infrastructure. We have discussions about cyber being used by terrorists. We see situations whereby cyber is used for crime or espionage and obviously we are also very well familiar with all the geopolitical tensions whereby cyber and the use of cyber technology has been used to let's say advance a particular political objective.

So, what has changed? What has changed is really the fact that on one hand, we have a massive amount of incident as it was previously mentioned, a massive amount of Cybersecurity incidents which fundamentally demonstrate the importance of being able to protect data

and the infrastructure. Incidents that show us why we can suffer damage.

On the other hand, we have also a massive amount of data. So think about it, the way you would think of how many pictures, digital pictures did you take last year, and how many do you expect to take next year? You know what? How that gradually increases more and more. Eventually, the amount of data that we as individuals develop, that we as individuals store, as well as the amount of data that we as organisations develop and store, result into one having a massive amount of information, but on the other hand, making the job of the security professional extremely more difficult. Why? The more data I need to secure, the more resources I need. The more resources I need, the more footprint of data have the more likely is the possibility of a breach, the more difficult is to protect everything.

I think it was Napoleon the one that said, the one who defends everything defends nothing.

So we can't defend everything even if we would like to.

Because on the other hand we have got all this amount of data, we have also massive more avenues of access, we are able to access information much easier and in

that a unprecedented scale. It is through this ease of access that we end up having value. Data is valuable. How many times have you heard that data has become the blood line of modern economy?

Well, guess what? If the data is valuable, if the infrastructure in which the data run is also valuable, then it should become, it should come as no surprise to us that it's going to be regulated.

The market recognizes that. The market recognizes that because, you know what, consistently, we see that being able to demonstrate a privacy, security friendly way in handling the data is becoming a competitive advantage. It is becoming something that customers, that consumers expect and want. Back in 2015, I'm pleased to say that I was personally involved in the development of a study by Symantec that was named the state of privacy report.

The state of privacy report was researching the behaviors and attitudes and expectations of consumers in Europe around the issue of privacy and data security. We reviewed in 7 different European countries around 7,000 consumers. The results were stunning at least in several ways. But certainly, also one that made a particular impression to me. If you would list all the

criteria that consumers would choose on the basis of which they would transact with a company on-line, 90 percent of them, 88 to be precise, would choose as number 1 criterion security and privacy of their data.

As a matter of fact, if you would look at it from a more humanitarian or from a more communal perspective, the fact that only 56 percent would care for the environmental footprint of the company that they would transact on line but 90 percent would care about the protection of their personal data, it clearly shows us that on-line we are selfish. We care for the protection of our information, as opposed to what may be the broader, the more communal good.

So have a look at that. But at the very least, it demonstrated to us that the conclusion was clear. If you could show that you were protecting people's data effectively, that you were securing the information efficiently, then that meant that you had more chance of doing business on-line, you had more chance of transacting with the customers.

Now, in the light of this technological change, reality change, even societal change in the way consumers perceive security and privacy, it's only normal that all also policymakers respond, that also they change,

and that they also take the necessary steps to protect what we said is valuable and therefore regulate. You know what, ladies and gentlemen, I think it's fair to say that data protection legislations around the world show up across the board, across different countries, across different jurisdictions.

I was in Japan last week and I was explaining to major Japanese corporations the impact of the European data protection legislation, and I was being explained what the Japanese data protection legislation in its refreshed version is going to look like.

I was having similar discussions about critical infrastructure in India roughly a month ago. I am immersed in data protection discussions in Europe quite frankly on a daily basis. Specifically for Europe, the latest standard right now and probably one of the most comprehensive regimes is the GDP R, the general data protection legislation, regulation, I'm sorry.

What is very important for me to stress here is that the GDPR takes a, in my eyes, a somewhat different approach in comparison to previous privacy regimes that we have seen in Europe, which has a long regulatory tradition in this area, as well as in the rest of the world.

Historically, data protection legislation has been about the protection of individual, protection of the consumer. To use a German term, for the right to information self-determination. I see I think a German speaker nodding.

Right now, the GDPR takes a radically different approach in the sense that for the first time we are talking actually about information governance. We talk about how you regulate the complete life cycle of information, from birth to death, from capturing to processing, to retaining, to securing, to what do you do when you lose the data?

This is why you heard all those concepts from the New Zealand data protection commission on the right to be, privacy by design, privacy by default. I often joke about security when is comes to Europe and privacy legislation I say the 9546 the previous data protection regime the one that the GDP R will replace in 2018 had one article on Cybersecurity. The GDPR has about ten now. So exponential growth of why Cybersecurity is important.

This is where the policies are going. Quite frankly, given how successful the European regime has been in let's say setting up a model, we expect this to grow.

But at the same time we need to remember that innovations and these laws are not, innovation is linked to regulation and these laws are not innovation neutral. I'm not making a judgment as to whether they are good or bad.

You need to imagine innovation like walking down inside a dark tunnel. And as you are walking down the tunnel, you don't know where you will end up. But eventually, you will end up somewhere. The regulation is creating a path which you need to follow, so you need to turn right because the law says you to do so.

It is not necessarily a bad thing, that you will turn right. But the reality is that we will know that only when you reach the end of the tunnel.

It's effectively the equivalent of saying that in the global competition environment in which we all are, some will go through the tunnel and will arrive on one destination, some others will go through a turn because they have to, because that is what the law tells them, and they will arrive to another destination.

Which one will deliver the best economic advantage, which one will deliver the best technology is something that quite frankly we will know only once we get there.

So and in my eyes back to the original question, is it a pull, a push, technology drives regulation, is

it policy, it's both. It's a pull and a push. We will only know what was then net economic outcome at the very end. But the reality from my end is that we will continue to see that trend very much, because the more cyber is becoming political, the more these two will continue to interact with each other. Thank you, Chairman. And happy to take any questions.

>> BILEL JAMOUSSI: Thank you very much.

(applause).

Thank you very much for your views and perspective and sharing your experience on this topic, and also how the data protection in Europe, the legislation has moved from one article to 10. Your point about, from privacy, security friendly technology, how we put that in place, and especially very important point about our days of the Internet of Things, and the data generated, and that data is the value.

We need to work on providing standards and technologies that will allow us to use that data with different perspectives of privacy. Thank you.

I'd like now to invite Mr. James Kilaba, Director General of the Tanzania communications regulatory authority, to share his perspective from Africa.

>> JAMES KILABA: Thank you, colleagues. At any ICT

discussion platform like this, we normally refer or need to joke about ICT related services, devices, growth, subscription, all users, network, signal coverage or even revenue assurances, and revenue generations, but today, as I say we are discussing the impact of emerging technologies on security, privacy and trust in ICTs. Why all this? Perhaps I could say, to me is the technological shift from an old Internet dominated by personal computers, we normally call them PCs, with wired connections, to the current with mobile devices connected by wireless signals.

This has facilitated more access to communications and extension, or by extension, we can say have created more access to Internet, and therefore to the cyber world.

So this could be the main cause of why we are talking today these topics.

Again, it is about ICTs related to services, devices, growth, subscriptions or users, network and signal coverage. My colleagues are talking about some of this in detail, but what I could say is that imagine technologies in ICTs has touched literally all these in total, and they play a central role on security. Why security? We need security for networks, security for systems, security for devices, security for datas they

have saved and even security for users themselves.

But we need privacy and the privacy ranges from users themselves, it goes to the data which are being conveyed, but again, trust, we hope to have trusted networks, trusted systems, trusted devices, trusted data, but also we need to have trusted users.

So, from all this, what are we talking about as regulators? It is about the challenges which are brought by people. So the central of all these are people. Without people, we could not talk of security, privacy or even the trust we are talking about.

So the role of users and their devices, irrespective of where they are connected, where they are fitted, or even where they are being used, is central.

We need to address that as we convene, as we get together as experts at a global level to address these aspects which are surrounded by effects and impacts of users and also devices which has been evolved from the old version to the current version.

Now, we are saying, back home, and at regional level, we have attempted to do a lot to address the security issues, and this includes even implementation of computer response teams, but we have also data centers built which are also and are going on how this old infrastructures

can be secured properly.

We are talking about people who demand all this, but we need you also to consider that around the globe, we have a high cultural diversity, but again on technological point of view, we have technologies like IoTs, we have machine to machine communications, all these require regulatory interventions especially in the resource segment, for without it we may fail again on the way.

But again we need to consider as we talk of security, privacy and trust that there is also time zone differences. This affects, as we talk of all this around the security, especially on data, on content and etcetera.

So we need also to recognize that to have a good approach to address this, we need to have harmonized standards, harmonized approaches on how to take into account that we have the diversities in our culture, we have the time zone differences, and even we have different expertise in how to handle Cybersecurity issues.

Such regional level we have our east African subregion where we have a collective and coordinated efforts to address this Cybersecurity related issues collectively.

But still, as it is well-known this goes beyond the borders. The east African region alone may not fulfill the desire and the need of combating insecure practices in our networks, and even carried on our devices. So the efforts at this global levels are important to us, so that we may come up with a globally agreed harmonized policies, and even whatever means we may take by taking into consideration the diversities we have around the world.

So, colleagues, it is our turn, it is our role to play, so that all this which seemed to be challenges can be mitigated but at a global understanding and levels.

Thank you very much.

(applause).

>> BILEL JAMOUSSI: Thank you very much for sharing your perspective from Africa, from Tanzania and also from the east African subregion, in terms of developing countries and the regulatory challenges faced in the context of security, privacy and trust in ICTs. That's very helpful. Thank you very much.

I'd like now, ladies and gentlemen, to invite the data privacy commissioner in Tunisia to share with us his perspective on Tunisia.

>> Thank you, Chairman. I'd also like to thank you

for providing Tunisia with the honor of taking the floor today, taking the floor today. We won't touch on the programme. But following the Chairman's words, following the concern of the international community with regard to this issue and also the conference held in Marrakesh last week, I'd like to say that Tunisia is responding to this international concern. Tunisia is a leader in the region an has been for some years, since this trend was affirmed with the constitutional revision of 2002, so well before the Tunisian revolution, since we made the protection of personal data part of the constitution in 2002 under article 9 of the constitution. This trend was confirmed with the new constitution in 2014, wherein, in article 24, now guarantees the protection of private life and personal data. But to the constitution which we now have, went even further, because we now have article 32 today, which enshrines the right of access to information and to networks with Tunisian citizens.

Of course this does cause problems with regards to the application of these principles, but it is affirmed in the supreme text of Tunisia now. We also had a leading text in our regions, since we had an organic law of data protection which was implemented earlier, and which

requested the accession to convention 108 of the Council of Europe.

This also with the African convention on Cybersecurity and data protection, all of this demonstrates the importance that Tunisia attaches to establishing this space for trust between citizens in the state but also between citizens and different economic operators in this area.

The Tunisia did not stop there, because we believe that access to information is crucial for data protection. We have legislative text, and we have had it since 2012 on access to information, and it's the new law on access to information which is the first text from the region on this area. It will enforce in March 2017 -- and will establish a instance body which has power to regulate and control access to information and check on it.

Things are really moving. We are really changing the situation creating this space for confidence. We did this particularly through acceding to convention 108 of the Council of Europe because we believe that data protection and creating this space of trust hinges on a national framework to go further, and expand this trusted space on to the international level through regional conventions, such as the Council of Europe

convention 108 and also the African convention of which I spoke, that the United Nations Special Rapporteur said, what we should begin to participate in drawing up a international framework for creating this space of trust.

This is a long path to take for our country which is a developing country, also African country but a country from the southern Mediterranean which seeks to ensure greater confidence in security for exchange both on a national level and also internationally. Thank you very much.

(applause).

>> BILEL JAMOUSSI: Thank you very much, Mr. Kadez, Chair of the national data protection authority of Tunisia, for your outlook on the rapid changes in Tunisia in the area which we are speaking about, and the changes in legislation and accession of Tunisia to convention 108, which improves data exchange.

Once again, thank you very much for having participated, and for having made the effort to be with us here this morning. Thank you very much.

Ladies and gentlemen, it is now time to open up the floor to you for any questions, you can ask your questions through the microphone for pressing once on the button, and then you will be given the floor. Do

you have any questions? Are there any questions from the floor.

I don't see any questions. The Chair is reminding me that we are a little bit late. So we do need to catch up a little bit of time.

I would just like to ask one or two questions of our panelists.

If there are any other points, of course, you can clarify them. I will begin with Mr. Ilias Chantzos. Measures are in place that facilitate the sharing of information between public and private sector on security threats and data breaches. Does it work, what can be improved, and how can standards help?

>> ILIAS CHANTZOS: Thank you, Chairman. Very good question.

There are two broad categories of measures. There are regulatory and nonregulatory. In Europe right now, for example, under the GDPR, the general data protection regulation, as well as the network and information security directive, there are certain obligations to critical infrastructure providers or to companies that have suffered the security breach to notify, to provide information to the regulator regarding that breach and the effect of that breach, if that breach was significant

enough. There are certain thresholds to be met.

That is the regulatory requirement, and it involves companies that have actually, organisations that have actually been victims of cyberattack.

However, there are also nonregulatory measures for information sharing. They are public sector organisations which are inviting information sharing and cooperation about security incidents with companies from the private sector, with critical infrastructure operators, with security providers.

Usually, these mechanisms are on the voluntary basis, and involve effective control of how the information sharing is done between both parties, and they also involve neutral exchange.

So the government department may be prepared to share information about an incident it has experienced, on the understanding for example that that information cannot go beyond the certain group of organisations or group of people. Equally, the private sector participants may be prepared to share information about a incidents they experienced on the understanding that this will be anonymized and will not go to their competitors.

So information sharing schemes like that do exist,

do exist at the national level in many European countries, and frankly, several of them work in very effectively. Standards are extremely important because it is through the standardized mechanism of information sharing that we can achieve both predictability, we can achieve scale and we can also achieve commonality of language as regards to what do we mean when we talk about a incident, what was the impact, and also what the mitigation measure.

>> BILEL JAMOUSSI: Thank you very much. That is very clear. Standards mechanisms for information sharing.

>> ILIAS CHANTZOS: And we participate in some of those.

>> BILEL JAMOUSSI: Excellent. I see Egypt asking for the floor.

>> Egypt: Thank you, Chair. Good morning, everyone. Very interesting discussion and very important topics we are discussing right now. In the beginning, I would like to thank Tunis for the marvelous hosting for this event. I would jump directly to my comment.

In the rush to monetize customer data, companies usually risk diminishing trust the users have in their products and services.

I was wondering on the views of our expert panelists whether trust have more value than customer data.

>> BILEL JAMOUSSI: Thank you very much for that question. Any panelist would like to take it?

>> ILIAS CHANTZOS: Without wanting to monopolize the discussion, first of all, you cannot do business without trust or at least without some level of trust.

So as far as I'm concerned, losing the trust of your customers is the worst possible thing that can happen.

Now obviously transparency is an important ingredient into building trust. Actually if you follow the next panel that I'm moderating, I will raise that.

But you need to be able to achieve transparency and how do you achieve transparency? You achieve it by explaining how you will use the data.

I'm sorry to say, but because there is no such thing as a free lunch, some companies have as their business model, and I stress some companies, have as their business model to offer the services for free, but to use the data in order to monetize and make a business model out of it.

I'm not here to represent the entire private sector. So I hope you understand why I'm insisting on the, some

companies. But the reality is that this is how the market right now operates.

From my perspective, trust is extremely important, but in order to build the trust, you need to be transparent about how you use the data. It is very often the failure of being transparent. It is very often putting it in the small, in the fine print and clicking next, next, next, that results into that loss of trust, which is ultimately bad for business and bad for the whole of the industry. And frankly, for us that are not in that industry, it's unfair.

>> BILEL JAMOUSSI: Thank you very much. Mr. Edwards would like to comment on that, please.

>> JOHN EDWARDS: Thank you, it's an excellent question, because whatever difficulties that we have had in this area is that, it's difficult to put a economic benefit on privacy. There have been behavioral economists have done excellent work on this, but when we look at the balance sheet, as you say the rush to monetize has a immediate benefit for a company for maximizing the value of customer data, and no direct information about the value on which the customers put on the data and their trust. We are fortunate or unfortunate in recent years to have had some good examples

of how customers value data, when things go wrong.

We have seen very tangible economic losses to companies who have failed to protect customers' data and have breached that trust. One is Target which suffered a significant breach. In the months afterwards, it saw hundreds of millions of dollars wiped off their stock price. The other is Ashley medicine, which is a case which may be familiar to many of you, a Canada based company, based on illicit dating which was subject to a breach, and again its prospects for IPO were wiped out when the breach became known.

What I think the reason, one of the reasons this topic is so high on the agenda, is that finally, it's not just a feel good thing or talk about human rights, that the bottom line to the business is really apparent, if you lose trust, you lose company value.

>> BILEL JAMOUSSI: Thank you, Mr. Edwards. I don't see any other requests for the floor. We are about half an hour late in the programme. So in consultation with the Chairman of GSS, we will recover that time during the lunch, because we have a two-hour lunch break. So we will shorten the lunch break and make it one and a half hours and gain time so we don't take it from Ilias Chantzos's session. It is now time for a coffee break,

that is complimentary coffee break downstairs at the garden area.

We will resume with the next session in a half an hour. I'd like to thank you very much for your attention, and for participating in the morning session. And I look forward to seeing you in half an hour. Enjoy the break.

(applause).

(end of session).

(break).

(standing by).

(Standing by).

(standing by).

>> BILEL JAMOUSSI: Ladies and gentlemen, please be seated. We are resuming our next session 3 that will be moderated by Mr. Ilias Chantzos. You have the floor.

>> ILIAS CHANTZOS: Good morning, ladies and gentlemen. Thank you for joining us in what is going to be I think a very interesting and very exciting panel.

I have already touched base with my coparticipants, and I expect that we are going to have a stimulating debate.

The title of our panel is, how industry meets end user expectations on security, privacy and trust, and

I have already indicated when I spoke previously about the kind of perspective that we intend to bring in the debate.

I think it's important to mention that when one is looking at the discussion around security, privacy and trust, one needs to bear in mind that trust is a component of every security, of every privacy discussion. Nevertheless, it's actually something that is very difficult to build. It takes a lot of time, and quite frankly, it can be very easily and very quickly lost.

As several recent examples ranging from disclosures about intelligence activities all the way to security breaches confirm us.

Also, quite frankly, I work now in Cybersecurity for 16 years, so it's very difficult for me to trust anybody. Okay? I mean let's face it. Part of being a security professional involves a certain hopefully healthy degree of paranoia of trust no one.

There are good reasons for that. There are good reasons for that. So, still, still in security and especially in discussions around public/private partnerships we speak about building trust. We speak about the importance of trust. We speak about small rings, small circles of trust. So how do we, these highly

paranoid people build that trust? What are the components that we need to look at? I would like to try to explore that in the discussion today.

I will very openly share some of the components that I think are critical, and then I will ask of all the panelists and most of them have slides to show you as well, so this will not be too technological and it will have beautiful pictures I hope, so I will try to identify what are the elements that one needs to consider when discussing about trust.

If I was to put my thesis forward and share it with you, I would begin by saying that trust can be built based on three separate components: Effectiveness, consistency and transparency.

When I talk about effectiveness, I talk about the effectiveness of technology, in the end this is about technology. This is a technology discussion. This is not about, for example, trust in a marriage. This is about how do we build trust in a technology.

In order to have trust in a technology, we need to be sure that the technology does what it is supposed to do, and delivers the results in an effective way.

So from the perspective of security provider, that means having the best of class technology, being able

to deliver the security result that the customers have bought and paid for, that the customers have voted with their money.

So be that with technologies like Norton, PGP, dot cloud, data lytic prevention, end point protection, Symantec is working hard to make sure that we deliver key capabilities that effectively protect our customers.

In doing that in addition we try to stay always ahead of the curve. How? By acquiring companies like the recent acquisition or trying to make sure that we will have the cutting edge R&D, also with in partnership with several governments around the world, that will deliver us knowledge and intelligence about what the adversary, what the cyber attackers are doing.

The other aspect is consistency, consistency of positions, consistency of where the company stands on different issues, and that can be around making sure that we detect malware wherever they come from but also about transparency, it's about being able to clearly articulate where we stand on data protection issues, where we stand on privacy issues. It's about being able to commit to customers on things like law enforcement access requests, all the way to things like we will return your money in 30 days after you bought the products,

if you don't like it, no questions asked.

It is about how you treat the customer all the way to how do you treat your, how do you discharge your responsibility as a responsible corporate citizens.

It's also about trying to make sure that your technology, that you participate in the public debate on cyber issues, which is for example why we are here, and also why we have done things like putting out papers on cyber norms and explaining why from our perspective, the technological integrity so maintaining the ability of a technology to function in a safe and secure manner are critical in building and maintaining trust in the cyber ecosystem.

These are the three components that I have identified, and we as a company identified as key elements in building trust. I'm sure there are more. I'm sure if you talk to other colleagues of mine, they will identify more. But I thought that distilling for the purposes of this debate this nontechnical debate, these three are key, are a good way of starting our discussions and are key, let's say, principles that can help us in this debate.

I'd like to start from my right-hand side, and I'd like to ask our first participant to take the floor,

to introduce himself and basically walk us through his presentation. Thank you.

>> Thank you very much, for putting these words and especially on focusing that building trust is one of the core elements for gaining the user's expectations and the user's requirements. I will try, I think we will need probably to switch to the first slide. Great. I will try in the next ten minutes or so to focus on the first point you just mentioned on effectiveness, as I believe that we need to cover Cybersecurity in a different way than we did in the past 25 years, to be able to pick up the real challenges, the digital economy of the future is going to face.

Probably just to introduce myself, my company, let me see if this technology is working. Great. Rohde and Schwarz is a company you know. As Cybersecurity is becoming more and more relevant we have started focusing on Cybersecurity in the past two years, and trying to do a similar contribution as we did in other fields to bring Cybersecurity to a level that it meets really the end user's expectations.

First of all, let me just start with some reminder that is helpful I guess for seeing how relevant the issue is we are discussing today about. If you see a report

from McKenzie two and a half years ago about the 12 most disruptive technologies, they are not only electronic or digital technologies, you will see there technologies like energy storage and so on, and the four most relevant technologies are indeed digital technologies. All of them are technologies that are addressed by Cybersecurity and by the topics raised on this conference today.

If I pick them up, you will see a couple of them and just to pick up one of them as an example, which is for me personally very interesting, it's big data. If we go back a couple of years ago, when I've been at university, there was a discussion whether it would be possible for a computer for artificial intelligence to beat a human being with chess. That was 1997. IBM just composed a computer to do so.

At that time, it was not possible. Ten years later, 2011, again IBM presented a computer and the answer was given to that question. So we have an increase in 15 years, a increase in power of computing by the factor of a hundred.

That gives us a possibility to do much more, that gives us as people are looking for Cybersecurity the possibility, but it gives also the people who are trying to do bad things and to utilize cyber to, in a criminal

way, also the same possibility.

Another point is Internet of Things. We have been discussing that for many years, and now it's getting real, as we have seen in the past couple of days, on Friday, where network devices has been able to shut down significant services in the U.S. East Coast, and with a denial of service attack.

These things are not more things we are only discussing in these conferences about. They are real. They affect our daily life in reality. We need to cover these.

For all of these, Cybersecurity is a basic enabler, as was said in the previous session, it is not a nice to have thing. It is and abler that is the prerequisite for many digital transformations we are looking on -- enabler. So without having solid Cybersecurity we won't be able to go and to utilize modern technologies that are coming with the digitalization.

I will give you a couple examples, not in a comprehensive way, more giving you an examples to show and to point on things I think that might be relevant for our discussion. The first one is information flow control information assurance.

You know the discussions about wiki leaks and prism

and others and recently also the disclosures from the U.S. presidential elections, and all of them shows that it is possible for a single persons, for single entities within large organisations even with very well secured organisations to transfer huge amounts of information out of this. We need to think about how we will, we want to be able to protect information flows in our organisations in our companies to address these threats.

A second channel are vulnerabilities. I think all of you heard about that, even if you are nontechnical, and this is a real issue. If you see just to give you examples of vulnerabilities, they affect standard applications, browsers, office environment, .pdf, your whatever you use. It is nothing you can avoid. You need to use them. We had the issue that the traditional Cybersecurity ICT security tools we are using, they are inherently not able to address these challenges.

So they are a new class of attacks. We need to find other models, other ways how we can address these kind of attacks.

Yeah, so we will skip that. The other thing is we will see new business models, which are increasing the threats. To give you one example, in Germany, the number of bank robberies decreased within the last ten years

by 90 percent. We have 90 percent less bank robbery, which is probably a good thing, but it comes not because the people are getting more, turning to the good side. It is because they are changing their business models.

You see there are not a lot of cash around the world. Now the people are moving to electronic payment. So the criminals are doing as well. If you see a couple of examples with that, you will see, we saw a lot of -- oops -- now, we saw a lot of, or several hospitals in Germany which has been attacked by criminals, that encrypted with ransom ware data, serious data, relevant data of hospitals, and caused a shutdown of the hospital for several days, and asked for money to release the computer and the IT system again.

This is a new model. The model works within economic framework, with a collaborative ecosystem. They have a lot of money to pay professionally, highly professional people to go through. So we have a model which is similar to the drug trade, and with a lot of economic strength in the background.

So we need to address that as well. Another interesting point is, and this is for a lot of people not really obvious, but it's getting more and more relevant, we have a lot of collateral damage. Everyone

was now browsing in the Internet, he is prone to be attacked by visiting servers, for example, that are infected, that are not targeted attacks. Nobody is trying to steal money from somebody like that.

But he will get a shutdown of his system as well after such an infection. We have a lot of collateral damage, and this is imposing significant economic damage to the whole society.

The question is now we have IT security for almost 25 years, what's the reason we are still having, facing these issues? If you see a little bit about the curves, how it approached, so we had since 25 years more and more tools using, we have antivirus, web proxy, firewalls, whatever, and the number of incidents didn't go back. They increased. We need to see that this is something which is not going to work out with a traditional approach. We need to think about new approach, to be addressed.

To give you an example, why this is the case, and this is a more technical example, but it shows that things are nontrivial. For example, we have in a standard programme that we say that this is a stable programme, we have almost a half, 0.5 crucial or significant bugs in such a programme. That means if we have a operating system with 40 million lines of code, we will have

something like 10,000 or 15,000 errors. These are ten or 15,000 errors that can be discovered by bad people, by malicious people, and try to build from these vulnerabilities exploits that can be used to attack a system. It will never be possible to have a system which is a hundred percent secure however, whatever you do before.

We need to explain in a analogy very good, what we have today is something which is similar to a Arabic method in the car industry, so if something happens, it does not hurt very much. But what you want to have is something like an ESP strategy, we want to avoid that accidents happen at all. It is a fundamental change in the way we address these kinds of threats.

Two things. So I just proposed three paradigms, I think what we need to do, it might be interesting for the discussion. The first of all, we need more proactive measures than reactive ones and also again in short example, it's similar to the ship industry, a hundred years ago when they introduced compartments to prevent and even if water comes into the ship, it is not risking the sinking the whole ship. We need to do something similar with the IT industry.

The second one is we need to go more for information

flow control, rather than access control. The third thing is again to the users, we need to leverage the users from responsibility they are not able to take by, because we know that users will never be as security experts, nor the network administrators will be, users will never be ICT security experts.

I will skip this.

And I will get probably to the conclusion. Cybersecurity, I think that we know all this. Is it getting more and more critical for the future. But we need to stress that. The currently deployed security tools are not adequate to address these challenges we have. We need to define new set of standards following a paradigm of the shift in IT security to cope with the increasingly smarter threat environment. I guess that the ITU community can provide significant contributions there that, especially in the standardization factor, and in linking that to the traditional telecommunications community.

Thank you.

(applause).

>> ILIAS CHANTZOS: Thank you very much. I would like to ask now Dr. Thomas Kremer to take the floor. I kindly request of our translators their patience and

their support in giving us a few more minutes of their time than what is originally scheduled. Thank you.

>> THOMAS KREMER: Thank you, Mr. Chairman.

Ladies and gentlemen, the digitization is progressing and will accelerate further. Virtually every aspect of our lives perhaps as you know will be affected.

Whether it is at home, at work, at shopping or play, digitization is huge potential for making our lives better, safer, and much more comfortable.

The slides are not coming yet. Let me give you some examples. We have apps that motivate us to get more active and fit. We are more flexible at work with smart phones and tablets, we are not confined to our desks anymore, and can take our offices with us.

Production processes can automatically adapt to the actual demand and customer need. Customization is the next standard. Self-driving cars are entering the market. In a smart city, you don't have to look for free parking lot, because your car already knows. But it's not all about comfort.

A self-driving car will help to prevent accidents, and to reduce a number of victims.

Because machines are never tired, distracted, or

drunk.

And these are only examples. The way we interact with machines or computers is changing, and it is for sure that there will be problems or mistakes, such as the Tesla which crashed recently.

Technology is not always perfect. But in the end, the benefits will by far outweigh possible risks.

Nevertheless, many people are worried about digitization and the collection of data, especially personalized data.

Who owns my data? Who is allowed to use it? Who knows what about me? What happens if systems are hacked? Six out of ten Europeans do not trust telecos or Internet service providers, and 7 out of 10 are concerned about their personal data being used for a different purpose than the one it was collected for.

Also in the United States, survey conducted by the national telecommunications information administration now show that citizens have concerns about unregulated development of digital business models. These citizens tend to use the Internet less. Overall, this could become a big challenge and it demonstrates that trust is crucial for the success of the digitalization and future business models.

We need to find ways and solutions to foster people's trust in digital business models.

So what can a private company do? We are convinced that we have to foster people's trust in digitalization and digital business models. We call it digital responsibility.

Digital responsibility means that we have to think about the bigger picture. What are the benefits, what are the risks for our customers? Assuming digital responsibility is nothing that we as a company can do alone, it requires a commitment of different players in different ways.

First of all, the legislators must ensure that there is balanced framework for privacy and data security is put in place. Data protection and Cybersecurity must be developed and embraced internationally, on the basis of jointly accepted standards. Many countries around the world, be it in Asia Pacific, in central South America, in Africa, have now realized that digital is not feasible without rules.

Europe has made an important step forward in this respect. We see adoption of the general data protection regulation earlier this year. And for the majority of European citizens and European business community, the

harmonized approach, the European approach is the personal data and security is a welcome development.

In addition, the business world and especially the teleco companies have to ensure a high level of security in the networks. Data protection guidelines should be implemented in a trustworthy way. Treating people with respect must not be compromised.

Only if people trust businesses, they will continue to allow their personal data to be processed.

New digital business models will lead to very complex data flows and processes, and the individual will struggle to understand. It will be difficult to determine who has permission to access the data and what they may do with it.

So, it is crucial to inform customers clearly how their data is handled. And they must not be left with the impression that they don't know what is happening below the surface.

Transparency is one prerequisite to earn trust and ultimately users' and customers' consent for collecting their data.

Consent is the main instrument for individuals to express their autonomy, that should be preserved for the digital world. But it is also crucial to find a

balance between the data protection and the need to process data for reasonable business purposes.

We at the Telecom think the best way to offer users is to offer users IT tools and apps to manage their privacy preferences across services. This can be done by using data dashboards or data cockpits in which privacy related information is summarized on a single portal, and users can check and manage their privacy settings at one place.

Both could simplify the consent process and help users to decide whether or not to provide consent.

At a lot of digital business models do not require processing personal data, for example, if you wish to improve public transportation planning, you do not need to know exactly who is traveling. So why should the data actually be possessed as data that is still related to persons. In such cases, normalization and standardization of privacy alternatives do not require users' consent on any case. Especially in this context, universal standards could be powerful leveraged factor.

Another powerful tool for users to safeguard the digital autonomy is encryption. The challenge to overcome is that there are not enough simple and easy to use encryption tools, so that in most of the cases encryption is only used by IT experts.

Ladies and gentlemen, security of computers and IT systems is crucial for safeguarding people's trust in digitization. This is by far not a new topic. But in the age of digitalization the numbers and the complexity of cyber attacks are rising every single day, and attackers are fast. We have seen attacks where in only nine minutes, attackers got the full control of the hacked IT system and make it part of an extensive botnet.

What can we do? Cyber attacks don't stop at national borders. Therefore, it's very important that the topic of Cybersecurity is thus discussed on an international level. Cybersecurity needs international cooperation. This means important international actors should work together, exchange ideas, and share both their good and their bad experiences.

Efforts are being made to strengthen Cybersecurity. Most recently, the European legislature adopted the directive on security of networks and information systems with the intention to establish a high common level of network and IT security. On this behalf we are engaging for common security standards and certification mechanisms for manufacturers of hardware and software as well as for network and service providers. But we

should not accept any proposal to furnish public authorities and security agencies with spare keys or vectors to its systems.

This would both undermine people's trust in digitalization and weaken security. Last but not least, simple and easy to use security solutions are crucial for safeguarding people's trust in digitization.

Security tools needs to be simple. Thank you very much for listening.

(applause).

>> ILIAS CHANTZOS: Thank you, Dr. Thomas Kremer for German accuracy in terms of time.

David, please, the floor is yours.

>> DAVID FRANCIS: Good afternoon, let me start by thanking very much for the opportunity to address this forum. It is a real honor to be here. Never thought I'd be addressing such an audience.

I'm coming at this from a manufacturer's point of view. I'm going to --

>> ILIAS CHANTZOS: Sorry, I'm being notified that we will have to continue in English only. Apologies for this. Please continue.

>> DAVID FRANCIS: It's because of my crazy accent. I apologize (chuckles).

As you can tell I'm Chinese, I work for Huawei. We are a global ICT company with 85,000 shareholders operating in a 170 countries, it is a good chance we are operating in your backyard.

We have 176,000 employees. When we think about security, privacy and trust, trust is built on people understanding privacy and privacy is only a possible if you got security in place.

There is about 200 of us in this room. And pretty much I think we can all agree what security looks like. Security we can sit down, discuss it and come up with a definition which meets everyone's requirements, and that is lovely. Privacy on the other hand, that is very different. If we just get ten of us in a room to discuss privacy we will come up with ten different definitions of what that looks like. It is driven by culture. It is driven by national history. It is driven by an individual. Often it's very personal what we deliver, what we consider to be private.

When we think about privacy by design, we need to take a step back of what are we trying to achieve? What we are trying to achieve is, to protect the user by handling the minimum amount of data, the lowest amount of data possible to deliver the best possible experience.

That sounds very easy, but that is not where we have come from. For 25 years, we have been running an economic model that says I'm going to capture everything. I have no idea why. But I'm going to capture everything. At some point, in the next year, ten years, 20 years, I'll figure out how I can make money for all this stuff I've captured. That's been the economic model for the last 25 years.

The world has changed. That is no longer an acceptable business model. The users are pushing back. It's changed. It's that definition of the minimum amount of data to get the best possible user experience is where we need to head.

How are we going to do it? You, my friends, you all play a key part in this, congratulations! You can all feel good about yourself. Because you can all go back to your home countries, and provide leadership, because that is the first thing we need. At a national level, we need leadership. An international level, we need leadership. You can provide that over the next two weeks as a start.

Second thing, as corporations, on this desk we will work for companies, we need to make sure that our companies actually have business conduct guidelines, that are

effective, that recognize the importance of privacy.

We as the industry, we need to do more. We recognize that once you lose user trust, you pretty much have lost everything. We have got to do a better job about security, as a start. We need security to be built in, not bolted on, which is the way we used to do things. That is the first thing.

Second thing, when we are thinking about privacy, we need to make sure that our staff are fully aware of what that means in a local context. Now I work between London and Brussels. I can assure you, that is who our journey between London and Brussels, you get a very different attitude on what privacy means. That little two hour journey means there is a difference. So I'm traveling thousands of miles. Why would I assume that privacy is the same in both places? It's not.

Therefore, we need to work in a local context, that local execution, this local understanding of culture is essential in the privacy landscape.

Next we think about the development aspects, and we heard John Edwards this morning talking about the privacy impact assessment frameworks. That is key. That needs to be part of normal behavior, how we conduct business, and driven the way we assess risk.

Then we need underlying principles. Firstly, no surprises. That's been touched on earlier in the day. People don't like surprises, either internally or externally. Let's make sure we have that transparency, there is no surprises.

A legitimate reason for what we do. We can no longer make it up afterwards. That is no longer acceptable. So being clear on what we are doing and why we are doing it. Next one, what we are doing is going to be justified. We need to have informed consent, not lists, huge long lists of terms and conditions, which are too hard to read. We have to think about an industry, how are we delivering terms that people can understand, so that their consent is explicit, not implicit in what we do.

Minimal data, I've already touched on that. Making sure the data is accurate, and it's the integrity can be ensured. How long are we going to keep the data? Am I going to keep the data for 20 years on the off chance that I might want to keep it? That it might be useful? Or do I only keep it for the time that it's going to be applicable and useful.

The last one is the most important one, it's that piece, responsibility. The industry needs to change its attitude. It's an important and fundamental issue that

we understand the data is never ours. The data never belongs to us.

The data always belongs to the end user. If we keep that in mind, that it's their data, then that changes the behaviors. It changes the behaviors of the staff, it changes the behaviors of our business models. That is how we are going to move that agenda forward.

We have some challenges. First one is, the users, the consumers. They don't think or behave how we think they should, or the regulators believe they will. The users are concerned about privacy, but their behaviors suggest they ain't that concerned about privacy.

They are still interested in features and functions. Privacy is pretty much low down their buying behaviors.

When privacy and security is the first question they ask when they are buying a handset, rather than how many pieces in the camera, then we will see a different behavior in the industry. The first thing is users don't necessarily do what we like them to do.

Second thing, as a industry, we can do a lot in making sure that we have appropriate security and privacy procedures in place. The consumers don't always like it. When they walk into a store, and we try and explain to them how we are going to look after the privacy of

their data and have they done this and that and the user screams, I just want my phone fixed! And I want it fixed now! It doesn't help that the industry have put all these lovely measures in place to make sure we look after their data. We need to do a better job of educating our staff, in handling angry customers, in making sure the customer is educated so they don't get angry in the first place.

Two minutes. I'm aware of that.

So, need to think about the laws and regulations that we have, and think about are they actually practical in the real world. I've talked about the cultural aspect, every country has a different view of what privacy means. That is going to change. One example of how privacy is going to evolve, at the moment the UK is rolling out smart meters. Right now I don't care if you know of my electricity reading in my house. But once it's available on-line, I suddenly do care. This data which I didn't give a damn about before suddenly, if you can read my meter in realtime, you can see that there is a pattern to my behaviors. You can see that I leave home on Sunday, I don't come back until a Friday.

If you can read my meter on a Tuesday and it hasn't moved from Monday, you got a fair bet, my house is going to be empty for the next three days. You can do that.

Right?

So, what we consider private is going to evolve. It's always going to be a moving, therefore privacy is going to be more dynamic than the security aspects.

So to close, privacy is going to be a journey. We are at the start. At the moment, if you go back a couple years, we were considering security. Then we moved into complying with security. Things like the GDPR were focused on compliance. This needs to evolve into operationalizing how we deliver privacy. And going forward, it's about making that next step where we look at what is the next generation of user really consider what is generally private and how do they want to see that delivered in the real world. Thank you.

(applause).

>> ILIAS CHANTZOS: Thank you, David. Now, Jaya.

>> JAYA BALOO: As the last speaker, keeping you from lunch, I'm going to try to keep it as short as possible. But it's a difficult subject. Please bear with me.

If we can start the slides. What I'm going to talk to you about today is quantum technologies, that is quantum computing as well as the challenges presented by quantum cryptography. Remember everything is quantum. We are going to talk about the problem and what are the

solutions, what are we going to do about it.

If you see the trend towards surveillance, digitally intelligence agencies have the capability to build a digital life dossier of anyone that enjoys the Internet. It means there is a lot of space for intelligence agencies to develop programmes to define how they are going to develop computing capabilities themselves. All intelligence agencies have a dual function, dual purpose if you will, they first have to make sure that they have signals intelligence gathering capabilities to break the communications of others and be able to read them in clear text. But they also have an information assurance directive which means they must be able to protect their own operational security of their own communication, and this is really the two programmes that are developed by the NSA, that describe how to use quantum computing and other offensive mechanisms to break other people's crypto.

What is this quantum stuff about? It is not a easy subject. If we think we know a lot about classical physics, there are characteristics we can consider, which is that it's happening of large things in the macroscopic world, it is deterministic meaning there is a action and there is a response. We understand that relationship between

the two. It's also quite intuitive. Quantum physics is quite the opposite. First of all, it is about the very small. It is highly probabilistic which means every time we are calculating what the outcome could be, it is really dependent on the role of the observer to see what is going on, and it's not very intuitive.

It also requires things to be super cool so that you can actually see the reactions that are happening between quantum particles.

Really, there is a lot of sayings that deter people from initially trying to understand quantum technologies, saying if you ever think you understand it, you actually didn't, but it is a really exciting area. I think that you as an audience need to do more than just the two words together to understand the actual opportunities and threads.

If you look, there are several properties of a quantum computer, the first is the fact that quantum computers don't use classical bits like we know it, which is a 0 and 1. They use qubits which could be 0 and 1 at the same time. If that doesn't start blowing your mind, I'm not sure if the rest of the slides will but they occupy this super position state, continuously -- qubits.

Next thing we should remember is that quantum particles have capability to have entanglement. Entanglement is a beautiful relationship, with two particles have a relationship with each other that affecting the one will automatically affect the other regardless of distance. This thing is the thing that gives quantum computing its scale, which allows it not just being 0 and 1 but also this entangled state can be thrown into the mix to add even more computing capabilities. It is also the thing that will allow us to build a new digital infrastructure called a trusted node network where you can define relationships based on the entangled state of different networks trusting each other.

The coolest thing about this is that Einstein said, I don't like this whole stuff around entanglement. It looks weird to me this kind of relationship. He called it spooky action at a distance. He didn't believe it. But most recently from the Netherlands at the university of Delft there was a loophole 3. A bell test prove a entanglement occurred over a distance of four kilometers. There were particles sent in opposite directions and when measured because they were entangled when affecting the one you could affect the other.

The other property you should imagine which is important for security is fragility and noncloning. When we are creating qubits they are fragile, capable of being destroyed at any moment. Keeping coherence is impossible. But also what is amazing is that there is a no cloning principle. If you tried to copy the particles, you will destroy them, by measuring them you have the potential to destroy them.

It becomes this capability of allowing us to know when we are being intercepted. Also it's not just the security aspect. It's the actual power that is being brought up by quantum computer. There are global implementations of a quantum computer. You will find they are not all created equal. You will see that we are trying to build something called a quantum annealer which is a slowly exponentially adding QU bits. You have a analog quantum which is a hybrid. The one that we want that is going to change the game is the universal quantum computer.

This is an arms race. The country that has universal quantum computer first that is capable of being viable enough to actually conduct the usage of algorithms that were developed a long time ago but require a quantum computer to be used, this is what it's about. Not everyone

can do this. We have a drawing up of our resources, of classical computer, which means that keeping on adding processing power to our classical computer systems will not be enough.

In order to look at challenges like breaking cryptography which is what a quantum computer will do, anything that is asymmetric, so all public key crypto system-like, systems that we deploy today are under threat by a quantum computer. If you use RSA, use a curve, you need to worry about what is happening in the field. The majority of the world uses this. In the EU there is a flagship quantum programme which pledged a billion Euros to making sure that there is an advancement in this field for Europe. Everyone is involved.

Are we there yet? The answer is no, because in order to have a viable quantum computer you look at how many QUbits do you need to exponentially decrease the time required to break the algorithm system. At the moment, we don't have enough viable QUbits in a universal quantum computer to be able to do this.

What we should do is, what do we do about it? We know we are not there yet but if a country gets there first, it is highly unlikely this information will be public knowledge. The assumption is in the meantime,

for our information assurance directive, there needs to be certain tactics deployed. The first and foremost, increase the key length of your current crypto use. The second is look at quantum key distribution, which is cryptography, to look for high critical links, what are the demands for long term secrecy. The third, invest post quantum cryptographic algorithms and determine how you are going to deploy them at scale over time.

If you look at the key length advice it is not just my advice to you, it is the NSA's advice that they have deployed as part of their suite B tactics to be quantum resistant in not too near future. They are recommending that everyone who deploys 40NSA -- for NSA must use quantum resistant algorithms. They are starting by increase of key length.

You should know in our traditional information security field, we talk about Al is talking to Bob. If Alice is talking to Bob over a quantum channel and worried about intercepting, we are looking for eve being present on the link by her trying to measure or copy. We go back to the noncloning principle. By Eve being present we know that link is not viable and whatever Alice sends to Bob is then corrupt. This is the easy slide. This is the difficult one. This is what it really looks like.

But I'm not going to tell you what this is about with the exception of telling you that those arrows in the middle, they require at the moment a fiberoptic cable, which has distance limitations of 64 kilometers, in order for Alice to talk to Bob that link can't be greater. We can't do global Internet infrastructure with quantum key distribution.

The word here is, not yet because there is something called free space quantum key distribution. There are trials that have been conducted in Europe, canary islands, which has shown that you can do free space quantum distribution between two islands with high powered lasers. We are seeing that the global development in China, for example, have a very large scale. The largest scale quantum key distributed network we have seen thus far.

This is where the world is going. They have launched their first satellite, that is capable of transmitting free space back to earth for doing quantum distributed node. Post quantum cryptography is the name for the future. This is where we should invest our smartest cryptographers, our deepest research. We have established our first quantum link. It is a toe dip in the right direction. But it is not enough.

In conclusion, we are just getting started. What

I need you to know is that there are public quantum computing systems available. IBM has basically launched a public quantum access platform with five QUbits and everyone can programme on. The information that is done on the system is intellectual property from IBM. After that Google is also busy. They are working on their own quantum supremacy experiment together with D wave. We are going to see a lot of things. What we need from you is a deeper understanding of what this means, because this could be the place where we have our next digital divide. Security will be only in the hands of those that can afford it, if we don't understand the threats of quantum computing and the options we have with quantum cryptography. We need to start now, if you want the entire planet to have some form of security that is not only in the hands of the few and those hands of the few will also be then able to do expert control over quantum computing technology strategies.

I urge you as thought leaders to take a step forward this week to actually look at how to make this type of technology more available to many. Thank you.

(applause).

>> ILIAS CHANTZOS: Truly fascinating. Ladies and gentlemen, are there any burning questions from the floor?

Because I'm told by our organizers that we are treading very thin on time. Is there anybody who is very curious or very brave that wants to ask a question from the floor?

If there are no questions, I would like then to thank very much the panelists, and we can break now for lunch. And we will continue the debate afterwards on the continuation of the panel, and I'll make sure let's say that also questions that are aimed for this panel can be addressed then. Thank you very much.

(applause).

RAW FILE
October 24, 2016.
1430.
HAMMAMET TUNISIA
World Telecommunication Standardization Assembly.
Global Standards Symposium.
Primary session.

Services Provided By:
Caption First, Inc.
P.O. Box 3066
Monument, CO 80132
800-825-5234
www.captionfirst.com ***

***.

>> Ladies and gentlemen, please be seated.

Ladies and gentlemen, please be seated. We are resuming the GSS. Ladies and gentlemen, please be seated. We will be resuming GSS.

>> BILEL JAMOUSSI: I hope you had a good lunch. We will be resuming the session now, session 3, how industry meets users' expectations of security, privacy and trust. Our moderator continues to be Mr. Ilias Chantzos. I'll give him the floor. We have one hour with interpretation, until, well, we have interpretation

until 5:30. But we need to stay within the block of time of three hours to be able to do this with interpretation.

So over to you.

>> ILIAS CHANTZOS: Ladies and gentlemen, good afternoon. I hope you have enjoyed your lunch. May I please kindly request that you take your seats so that we can get started as time is of essence. Thank you very much.

We are going to try to continue with the process that we followed in the previous panel, continuing the stimulating discussion.

I will ask of the three panelists to keep to the ten minutes time line for their interventions. Then what I hope that we are going to be able to do is have enough time to have both the panelists of the previous panel as well as the panelists of this panel meet all together and actually participate in hopefully what will be a interactive conversation about some of the points that have been raised.

I do hope that you will be brave enough to ask some questions, and otherwise I will volunteer the questions.

Without further ado I'd like to invite James Snow to take the floor. Enjoy the conversation.

>> JAMES SNOW: Thank you. Good afternoon, everyone.

Hope you had a great lunch. My name is James Snow, global security and privacy strategist for all of our Google cloud products at Google. This is all the products that we are selling to schools, to businesses, and to governments, and today I want to talk about what we see in the realm of security and privacy.

Let's throw some slides up on the screen here, if that is all right.

First of all, why is this important? Now, the problem sometimes with standards is that standard moves very slowly but innovation moves very quickly. At Google we are seeing hockey stick growth across all of our different platforms from storage to core compute to engines. But I'd like to talk about how Google addresses security.

Hopefully we can throw a couple slides up there. There we go. Fantastic. Loving it.

Let's talk about what Google does. What you are looking at is a picture of one of our data centers. Google takes security so seriously that we are one of the few companies in the world that handles everything from end-to-end, on any given day we are the world's third or fourth largest manufacturer of servers in the world. We make everything from the chips to the mother boards

to the proprietary operating system all the way down to the application stack.

The idea here is that we are not going to be subject to vulnerabilities from third party suppliers or third party solutions. If you stepped it up to network, so this is ITU, let's talk about network, Google also builds and maintains our own network equipment, we manufacture switches and routers, we make proprietary communication protocols and rotate these.

On the left or right-hand side, big picture is one of our Jupiter super blocks. This is what we do just getting started.

All of that equipment is actually connected to what we believe is the world's largest global IP network. This is not just a network that connects data centers to each other. This is a network that connects our data centers to nearly every ISP in the world. This includes cables across the Atlantic and Pacific, we currently have over 13 but we are building more all the time.

When we talk about network points of presence, we have locations in 77 different countries. We have over 849 different edge nodes. We want to talk about performance? If you are running a VM on our infrastructure and it needs access to high bandwidth

networks, we can spin up a connection that can provide a million QPS a second in less than a second.

Extraordinary, high performance computing. When we talk about spending money, this is expensive. In order to be able to do security all the way from the chips all the way down to the network, this is a massive investment from Google. Last year we spent almost $10 billion U.S. dollars just on our infrastructure alone.

Let's talk about our infrastructure, another picture here, this is something that we are growing, we are adding regions and data centers. We are looking at announcing one per month for the next year, including new cables that are being built out.

We are very much in the Telecom business. When we talk about what makes Google different from a security perspective, it is just basically this. No one handles everything from the chips to the mother boards to proprietary networking equipment to the world's largest network to the application stack, all the way down to the mobile clients.

From a security perspective, end-to-end is the only way you will be able to protect your infrastructure. We had to move very quickly, because we have been under

constant attack by individuals, by governments, almost since our inception.

But not only is security important, we also have to talk about scaling security. At Google we have had a dedicated security and privacy team now for almost ten years. We have over 600 of the industry's, some of the best professionals working there. This isn't just the smart college grad of the moment. This is the inventor of Linux.

We are spending over two billion annually, in addition to 10 billion that we are spending on security itself. I'll talk about investments we make there. In addition, there is a lot of smart people in Google, but they are even more smart people outside Google. We are collaborating with the research community, and education. Last year, to date we have over 160 research papers on security that we have published.

Google, you may not realize it, was the first large Internet provider, first large Internet company that had a bug bounty programme. You as a company, as a individual can run a pen test against our software or any of our solutions to prove how strong our security is.

We operate at many different levels all the way

down from the handsets to on-line collaboration suites, to infrastructure and software as a service. We have now moved into offering advance machine learning. There is a huge market out there.

When we look at data protection, the way that we store and protect information at no point in our infrastructure is any data in a unencrypted format. When you connect to Google, you are connecting over a very strong encrypted connection. We have, we are one of the few companies that has a quantum computer. We can tell you that we are developing cyber suites that are beta, in beta today which you can try which are meant to defeat the future threat from quantum computing that we learned about in our previous presentation.

A lot of these services are growing quickly, up until now we have over 28 different services focused on everything from analytics to application development.

The most important thing to realize is that security at scale has to operate. At Google we have I believe 7 applications or platforms where we have over a billion users every single day.

Being able to provide this sort of infrastructure and information in a secure manner is paramount for us.

When I talk to companies or individuals about

security at Google, we usually blow them away. Most of them don't realize we are doing all this work. But the conversation quickly turns to data privacy.

You are Google. You guys are good at processing information. Why would I trust you with this information? Here is what we want to talk about, we have two different solutions for two different groups of customers.

For our consumer business, the things that we offer for free, we are using this information to train our machine learning to do advanced spam detection, for tweaking and tuning of all our solutions.

For our business customers, we are able to utilize that data that we gather in the consumer space and apply those protections to our business customers so we don't need to process business, government or student data. We can actually respect their privacy and not use the data for any purpose other than what is intended.

We very much support the idea of transparency. Google is also one of the very first companies to have a transparency report about what services are available. Government requests, what is being used for what sort of purpose.

We want to empower people to make good decisions about platforms and solutions before they ever become

a customer. You would like to know datacenter locations, how strong our encryption is, our contracts, our availability? All these things are publicly available, not just to you as partners, but also to customers and to citizens.

It's very important that all services follow the following sorts of steps, which at Google we like to pioneer saying we are going to tell you what we are going to do with your data. We are going to commit legally to what we do with your data. Most importantly, how do you know what we are doing with your data? The idea is we can only use the data that you provide us to provide the service that we are providing. If you are a business who is using gMail or compute engine, we can only use that data to provide a service so no profiling, no advertising. We can't even use that data to improve our own services.

Intellectual property of data put into our cloud belongs to that of the customer. Google has no rights under any circumstances. Last but not least is port ability which we have talked about today. But in cloud computing, this takes on a new idea. Earlier this year we open sourced a solution called Kubernetes. The idea of having computing you can dynamically move from your

data send to to our cloud, to Amazon cloud, Microsoft cloud, on demand. If someone has a better price or better availability or there is an outage, you can dynamically move between all these different environments and this is what is going to be empowering your users. Actual having true portability of information.

Contractually, this is also important, because we operate globally in nearly every country. We need to meet the strict data protection requirements that are in those regions.

Everything that we do at Google is written in the language of the European data protection directive, where the customer or the consumer is the data controller. That means they own the information. They instruct us, the data processor what we can do with it. We simply cannot use the data for any purpose other than what they have simply instructed.

When we talk about data privacy, Europe comes up because Europe has been the pioneer in this range. Data privacy in Europe has been evolving. When people refer to privacy now, they are referring to the European data protection directive from 1995. This had restrictions on what you can do with European data and where it had to reside. This is evolved from moving data from Europe

to lawfully move it not just to the U.S. but other countries all over the world, as long as the correct security and legal protections are in place.

New developments like the European general data protection directive also enforce this sort of requirement going forward.

Last but not least, this is the most important part of any sort of privacy discussion, is that Google takes the position that, yes, trust is important and we have heard that word a lot today, but I would say that you should trust but verify. The way that you have verification is when a independent third party is able to come in and test your environment.

I have this broken into two categories. At Google we operate one secure cloud. We don't have a German cloud, don't have a healthcare cloud. We have one cloud for the world.

That means that our security standards apply to that global cloud. No one gets treated any better or worse. We leverage the certifications from ISO. We do a lot of the classics, ISO 27001, the new one, ISO 27017, SOC 2, SOC 3. But this is security focused. We have new data privacy standards which you are embracing. My current favorite is ISO 27018.

Where ISO 27001 said Google drive is secure, or it meets the security requirements, ISO 27018 is doing an audit and saying, is access restricted appropriately. Privacy is harder because it's not just an application. It is every way to access that data. Any API, any add on, every client, so this is the sort of certification that we want to have going forward.

Last but not least I'm going to stay to my time which I'm actually pretty impressed with, I'm going to leave you with a closing thought. Although we can all go out and develop our own clouds, I think that my recommendation going forward is to leverage, we are all going to be living in a multi cloud world. That could be some from a local Telecom, could be some from a Google or Amazon or Microsoft. But you need to architect your solution so the data can move freely between all of them.

Doing business with the larger partners like Google and Amazon we do business in nearly every jurisdiction in the world, which means you are always going to be getting the highest standard, whether that is data privacy from Europe, healthcare protections where the U.S. is leading, or encryption requirements from South Korea where the regulations are also quite strong.

With that, I'm going to say thank you and I want

to make sure we have time for other speakers. We will answer any questions in the Q and A.

>> ILIAS CHANTZOS: Thank you.

(applause).

Dr. Du.

>> YUEJIN DU: Thank you, moderator. I prepared a presentation for 20 minutes. However, the moderator only tell me we only have ten minutes. So if I cannot make good presentations, as a fault of the moderator, so today I want to share with you what has been done in security and what our reviews, security, is world is changing and we are talking about security of only those who can adapt to the change can survive. How the world is evolving and changing. There are three critical things. One is data, Internet and computing powers are changing the world. With the three together and some people say data assets are era into ICT data, the big data market world will reach $128 billion in 1980. Data is everything of the future to take Alibaba as an example, we have curated a Chinese single stay or bachelor stay global shopping festival. Last year on this very day, the total transaction value was 92 billion yen.

So actually, solo transaction can be done in very few seconds, and the transaction must be judged whether

feasible or not within milliseconds. We also can make a decision whether we can then launch to the SMEs without any humans intervention, and 70 percent of the largest companies have access to Alibaba's platform. There is no logistic vehicle, and why it's logistic companies wants to access the platform, because data behind can help them improve efficiency. Data is magic. That is also the power for Alibaba and innovations are sprouting up in China, and the data is behind all of this. Data is like the Oreo and the data is everything, is critical for Smart Cities, health, education, manufacturing, and everything will be changed by data.

Data is so good, so nice. However, data can also be evil.

You can see on the left-hand side, there is a little girl, and she died in August because of heart attack. And we have been discussing this in China, and it was a piece of very hard news, and this is a result of the Telecom fraud. Many received the diploma, the offer from the university, and actually she was, her money for the college entrance was actually deceived by the Telecom fraud.

For many people, it is not big money, but however, for this family, it's big money, and which result in

the heart attack. So there are so many such things happening in China. There are six government ministries in China, working together to fight this.

You can see the Chinese police are working with other police agencies to actually bring the criminals back into China, and there is also an estimation in China, in China the estimation is that those people in the gray market is 400,000 to two million people doing this type of things, and they are highly organized.

People do not reside within China. Some actually are located in southeast Asia.

And each year, they can generate 100 billion revenue. Actually this is a loss for other people. The Telecom fraud has attracted attention from the people, and I think this is caused by the information or data leakage, and once the sensitive information is disclosed, the Telecom fraud cases can actually find easy target.

It is not only happening in China. It is also happening in other parts of the world, the data leakage. That is from data or information is built from website and then the enterprises or governments, their data are stolen. The data can be used by the criminals which may result in huge loss.

On the right, you can see these are the reasons

for information leakage. There are so many differences, the reasons from hackers, the reasons from internal employees who sold those information, and the black market in China can reach 100 billion yen value. That means it can buy a lot of people. This is not only a phenomenon in China but a phenomenon across China so we love the data, but we also hate the data too either.

So some thing we do not want to see happening due to data, but we must admit that no matter you love it or you hate it, we need the data. We are entering the year of data driven technology, and I entered Cybersecurity era in 2011. And in the future if you want to win the fight against security, data will play a very important role.

I think that people will agree with the claim that security itself relying on data, and in China we say stop eating for fear of choking is never a choice.

We cannot neglect this issue. However, when people talk about data security, what type of data can be checked and what type of data cannot be collected, probably we should look at another more important issue, and if the data has to be in that other people's hand, how can we do better data security, because we have so many different type of data.

So I will talk about three aspects. First, what are the major threats, second, and today we need to protect the data, what are the major challenges, and what are the key message we have to adopt. Actually the key risk come from internal abuse, for instance, if a company has the data, and the data sometimes has sensitive information of the user, if you want to provide service, you need this data. The consumer on the Alibaba platform make a call and asking the service agent how we can help them to solve the problem, and that the customer agent can look at the data of this customer, it's fine. If the customer agents are service representative, look at the data of another people or another client, it's incompliant so it must be legally and reasonably compliant. And there are so many cases also, misuse. We need to use the data to generate value to provide more precise services for the clients, from the testing to the product delivery, to the data usage. We have a whole process verification, and no one person can actually touch on the sensitive information or the data.

And also internal staff may cause data leakage. We need to tackle those three challenges. However, old methodologies cannot be applied for today's world. And today we are more than static data which start on the

hard disk, it's more than a data record. Probably I will spend one more minute, and the data is everywhere, and the data is flowing, is changing, and data is in the services, and service is an eco, Internet environment. We need to protect data and search the complex environment so we create a method based upon our expertise and experiences, that is the data sent data maturity model, and this is data centric security. It's different from the system centric security.

I will not go into the details. It's a complete new methodology. It's like a new model. And we cannot do it alone. That is something we came to realize, the whole ecosystem need to have this capability and we do all this to win the trust and confidence of the clients.

This is efforts we did. And we have the model on the left, and it has become a project item. And the Internet has become an industry and national standards, and we have also promoted this model in the industrial associations. We also try to influence the decision-making and policies, and in one word I would like to conclude, we do all this to really enable data to bring value to us, and that Internet is a platform which can be used by both bad guys and good guys. Only one can have a very good use of the platform it can generate

value or it will lead to disaster. Thank you very much.

(applause).

>> ILIAS CHANTZOS: Thank you for being so quick, with his time and his presentation, and apologize for me being such a joy killer, but I'm afraid that this is what we need to be sticking to.

If I can have the clicker, thank you, Bernard, walk us through. Thank you very much.

>> Could we have the speaker's microphone, please?

>> BERNARD BENOIT: Can you hear me?

>> ILIAS CHANTZOS: Can we please have the slides on the screen? Thank you.

>> You have to love the technology when it's working and also when it's not.

(chuckles).

I love to see me on the transcript too.

>> Start talking a bit about what you want to talk about.

>> BERNARD BENOIT: I'm going to make this presentation in French, to really encourage linguistic diversity, without sticking to English. I'm going to present a point of view from an industry which is the Kudelsky group not widely known in the public sphere. Our main aspect is security. We will find it in 1951,

and today we are a global leader of integrated content for television.

The slides now disappeared from the screen.

Would it be possible to put the slides up on the screen, please? Marvelous. Thank you very much. As I was saying, background is the TV content protection, we protect more than 60 billion TV content per year, about 360 million devices that covers.

We have been doing this for about 30 years, and activities, the protection of physical access, parking, stations, we have developed since 2012 based on our expertise in television Cybersecurity activities as well.

I'm not going to go into real detail on this, because we are going to try and focus on content protection, on networks. Okay. Thank you very much.

What I'd like to do is to go back a little bit on to network and protocols. Today on the telephony networks we have 2G, 3G, 4G. Now we are beginning to look at 5G as well. We have an SS7 protocol which is quite old, which began in the '70s, and we have networks which are very heterogeneous, and by their very nature, cannot be the source of security. We often find flaws, and we cannot update these networks, it can't be the

base of the security, therefore.

To reinforce security over untrusted networks, a view which is based on our experience, is to have an approach which is independent of networks. Some people call this over the top approach. At least we have a layer underneath which is independent of the networks, it should allow us to have a security network. Our view is also based on experience. This can be a hardware security so it has to be a hardware element which is very specific, whose only functionality which is to bring security, and this is, has to be scalable, of course, to millions of users.

It also needs to be a cross platform approach which is independent, and it has to be on mobile or nonmobile platforms as well. And above all, it has to be compatible with the legal intercept. So what is happening at the back of the room?

I'll continue.

So, compatible with the legal intercept is a very important point, because our democracy will only exist if the law does not limit democracy, no one has, so we need to have a system which is very trustful, which is very important, but one must also have a view of the compatibility with the law itself.

So our proposal is a Swiss solution which was, which we launch next year which is going to secure voice and instant messaging which is, has to be support for all platforms and which will protect from point to point for dedicated hardware, the content protection, but also content integrity of messages, and user authentication.

I'm really not going to go into further detail on that. Our proposal is to bring national sovereignty back to countries. We see a lot of over the top solutions are for software today, are operating outside of countries. So this results in that there is a shrinking sovereignty from the states, and also shrinking revenue for local operators who see that their income and their voice is disappearing.

There is also shrinking revenue for states and for governments, which is regards to taxes. So our opinion is to bring back value to the operators, while also at the same time bringing back national sovereignty for the governments. By proposing a solution which is really managed by the local government, and is not outsourced from the government, so that is what we are proposing.

That is really a short overview of our vision. Thank you.

(applause).

>> ILIAS CHANTZOS: Lovely. Thank you. Very pleased to see that we have got about 20 minutes for questions and answers.

So, before we sort of like switch it to the panel, I would like to ask you if there are any pressing questions from the floor, for these panelists participants. In the meanwhile, I would like to ask the previous, the participants of the previous panel, if they would like to come up on the podium and we can do the debate.

So, the Chair recognizes the gentleman, the moderator recognizes the gentleman.

>> Thank you very much. Today we have listened to very interesting information. The speakers today represented companies, operators, and also independent experts spoke. In listening, we got the impression that everything is just great.

Then this begets the question in the future what are we going to have to do? For example, I was expecting the speakers to promote for the future some global international standards that I think is a topical issue. This is a question for all of the speakers, the very distinguished speakers. Thank you.

>> ILIAS CHANTZOS: Does somebody want to say something on global international standards? Please.

Du.

>> YUEJIN DU: Thank you Mr. Moderator and for your question. I didn't extend my presentation in Alibaba due to time constraints. The reason we have to do the standards and to invest so much to do such a standard is because data is leaking, is being leaked everywhere.

It is not that Alibaba can protect its customers because we can do our data good, we cannot do so because our ecosystem is highly complicated. When a consumer spends money in Alibaba there are many processes that are out of control by us. Therefore we also need others to protect data. This is why Alibaba comes today in hope that our practice can actually be of some help for others. We also hope that ITU can serve as a platform to diffuse our good practices.

Only by various companies and various sizes can do data well, can we truly have the confidence and trust as I mentioned in my previous presentation. I thank you.

>> ILIAS CHANTZOS: Thank you. I know that representative of Google wanted the floor. And also Huawei. Please.

>> Sure. We can take turns. I'd also like to strongly agree. I think the question about what sort of standards would we, are we looking for, are we lacking,

so unfortunately, many times standards and regulatory bodies aren't moving quick enough. For us, at Google we oftentimes have to innovate and do these things ourselves, but what I think would be most interesting or valuable is that when Google or Huawei or Alibaba find some sort of vulnerability or some sort of exploit that we could be able to share this in a more vocal way. Today we discover bad things all the time. But oftentimes we cannot share this, because just the act of a sharing this information somehow makes it our fault, or we could then be liable.

If I could make a gentle request, help us help you, by allowing all of us to disclose what we find out, when we find out, so you can protect your users. Thank you.

>> ILIAS CHANTZOS: This becomes a discussion of responsible disclosure in many ways. The question of course becomes, what is responsible, meaning how much time, how much opportunity you give for others to fix the patch, what does it mean in terms of the liabilities that you just laid out. Huawei also wanted the floor, please.

>> Fully agree with that point from the floor. There needs to be more international regulation. There isn't. We are not doing enough. That is why we came here today,

to make that appeal. From a vendor point of view, I'm sure that my colleagues have the same problem, is that because there is no alignment on standards, there is, the problem of standards, there is no standard. They are all over the map, which puts up our costs, which lowers the quality of goods that you have, and you can't compare one vendor with another, because they are all evaluated differently.

There is the how do we build things in the first place best practice type elements. I think we are doing more on that side. Then there is how do we evaluate what the security looks like. That is just all over the map. I think we made progress on the sharing of vulnerabilities. When we talk about sharing though, we need to distinguish between what are the threats, what are the incidents and what are vulnerabilities. Each of them covers, carries with them a different type of risk.

The threats, absolutely, we should share the threat information, as widely as possible, without putting fear of god into people. Incident elements, if you can anonymize, we need to do a better job of sharing that. We see different countries, mechanism being built as part of strategies to share information within territorial borders which is encouraging but not enough

is crossing borders. We have a vulnerabilities element, that is a different level of confidentiality.

If you have got one customer who is moving quickly and approach to patching and another that doesn't, is it right to put the other one at risk? There is a element of you need to have more control over vulnerability of information shared, otherwise you are exposing all the networks globally to the risks.

But yeah, absolutely there is an appeal to everyone in this room. We need to do more to get closer alignment on international standards, rather than national standards.

>> ILIAS CHANTZOS: I will give the floor to Dr. Thomas Kremer, he wanted to mention something on this. The only request actually I would make to the speakers, apart from them being brief, is also to highlight that, when we are talking about standards, what do we mean? Do we mean technical standards? Do we mean regulatory standards? Or do we mean performance based standards? When I'm speaking to a policy audience like yourselves, I think it's very important that we are very clear in what we are calling for, because all these are standards, but they mean something very different.

>> THOMAS KREMER: I'm referring to regulatory standards, and just keep us in mind that just this year we achieved Europe state of privacy regulation which gives us a uniform privacy law all over Europe, all over the 28 member states. What we consider is whether there could be a standard for a much broader applications, first point.

The second point is, sharing of vulnerabilities is from my perspective key, especially what we need is simply, we need patches as fast as possible, when a vulnerability is discovered, because we can be sure that any hacker and any attacker will get our vulnerabilities within a very short time period so customers could be hurt. That is why I think patches is very, very important. Thank you.

>> ILIAS CHANTZOS: Thank you. Other burning questions from the floor. Come on, don't be shy.

One, two, two and a half, three. Okay. You know what? I enjoy sometimes being provocative. I would like to ask a provocative question, since I know also that is something that has been raised in the discussions, we hear a lot about regulatory standards and we hear about, for example, what is going on in Europe around GDPR.

Yet, often we see regulatory standards that come together with specific localization, and I mean data localization mandates, requirements that data are stored in country.

I would like to ask actually the view of the panelists, as to whether they feel that these data localization mandates achieve their objective which is allegedly better information security or better privacy, or they function also as competition barriers resulting actually into reducing both customer choice as well as the desired security and privacy goal.

The floor is yours, gentlemen. Who would like to take this? Google, we will start from my right.

>> JAMES SNOW: I'll have fun with that. I hear this a lot when I speak to customers in industry and education and government, the whole, this whole term data sovereignty it didn't exist a year and a half ago. Does it mean that your data has a passport? No, no. It means that when people are trying to understand what sort of protection data has if it exists in a certain geography or another. At Google way that we look at this is that we operate a global cloud.

If you try to have a cloud that resides in a specific geography, not only are you going to have down sides

from high availability and high performance especially if your users are located globally, I think the question that we need to talk about from a regulatory perspective is how is that data actually protected? Just because you keep it in one country does not make it safe.

Hackers do not respect borders. To use a European example, the upcoming GDPR and the existing data protection directive all allow for the export of data outside of these geographic boundaries.

There are some types of data where this might apply. This might be military data, this might be something that is highly sensitive. When we talk about what sort of regulation should apply, it should be about data protection.

If there are questions around jurisdiction, these are things that are typically solved within a contract. For example, if there was a French company that was getting data requests from the Canadian government, the Canadian government should not have any rights to that information, if that company does not operate within Canada.

That should have to go through the local authority. There is a lot of confusing points, when we see data locations as a requirement, it is often not a requirement. We invite you to think about it in a broader sense, how

is your data protected? What law applies? How does that relate to high availability? Because we are operating in the global world.

>> ILIAS CHANTZOS: Thank you. I know that the representative of Huawei also wanted the floor on this. We will let him pour water first (chuckles).

>> I think we see a lot of good old-fashioned protectionism. We talked about in the first question, the need for international regulation, so there is definitely a need for international regulation around that. That helps have a more market which is the GDPR is about which is a vital step in the right direction. Often it is about a excuse. It is about having the right controls in place so you can provide confidence to the users that data will be appropriately protected. That doesn't mean it doesn't matter where it is. My problem with sovereignty, it gives the illusion of security. Because it's somewhere you think it is, then it must be safe. I think it can also lead to poor security because it's a illusion rather than real security tested mechanism.

>> ILIAS CHANTZOS: Another question that I've been discussing with the panelists, is the question of, and we heard actually an excellent presentation earlier on

encryption, the question that we hear more calls around encryption and around even how encryption needs to be stronger or even how encryption needs to be weakened in order to address public safety and national security objectives.

And especially let's say being European myself, and seeing the kind of terrorism concerns that exist in Europe, it's a debate that I closely follow.

I was wondering if the panelists around the table also had views to express. I see Dr. Thomas Kremer all right.

>> THOMAS KREMER: I assume you are referring to the issue back doors in IP system and if we implement a back door in a system it's only a question of time until hackers and especially organized crime will discover what is, what has been done and say with users. At the end of the day every back door will lead to the situation that we will weaken our security and this is a bad thing.

>> To add one thing, it's an excellent comment. To add to that, we are all the time talking about trust and this is a very crucial point. We cannot try or hope to get trust from the end user, and at the same time we tell the end user there is probably a back door into

the system we are not able to tell you about. This is not the foundation about trust and this is the basic issue we need to address in Cybersecurity.

>> ILIAS CHANTZOS: Please.

>> JAMES SNOW: I'm going to talk about the elephant in the room. The thing to talk about is part of the Snowden disclosures that came out where it said a lot of large Internet companies were somehow cooperating with governments, it depended on the cases. For example, in my presentation I talked about the fact that we had undersea cables across the oceans. When Google got hacked, it was effectively by both the U.S. and British government taking a thermo nuclear submarine under the ocean in international waters and tapping one of our cables.

That is illegal access. The interesting thing was is that when we discovered that this was happening we found out it wasn't just the Americans and the British. It was all kinds of governments were doing this. They all seemed to talk to each other.

What we saw is that encryption was an effective means in this arms race. After that, this is when Google started developing our own networking equipment, and advanced encryption protocols and all these things being

put into place, and make no mistake, there is a such thing as lawful access to data. If a country has a terrorism concern and you would like to find out about that individual, if you follow the proper legal path going through a court, companies will provide that information.

At Google we are pretty confident about this, after we put these controls into place, we have seen all those requests really increase because they are not getting their information going through an exploit or back door, they are being forced to go through the front door.

We think that the encryption, there needs to be more of it, not list of it. It needs to be evolving. This is something you should hold your partners accountable for.

>> ILIAS CHANTZOS: Another opportunity for the audience, if there are any questions you would like to ask. Otherwise I'll keep going. The Chair recognizes the person at the back, the gentleman at the back, I think.

>> Yes, thank you very much. Nigel at ICANN. Could I ask the panel, I found the presentations most interesting and stimulating, and certainly this question and answer session has been very informative.

We do read, when we read about massive cyber attacks and of course we have just been reading about one at the weekend, and we read about how users' computers are infected and how users need to take more care about what they do, etcetera, people talk about this, I'm just wondering what the panel thinks, because you are experts.

What can more, what more can be done at the user end, in terms of education awareness, should there be some sort of driving license for computers? I know we have been over this sort of thing before. But I'm wondering especially as we are now entering the Internet of Things and people are concerned, it is one thing buying a computer, another thing buying a control for your air-conditioning so to speak. Thank you.

>> Hello, Nigel. Very good question. I'm going to share the floor with the other participants, but I think I would have views on that particular as well.

I think there is certainly an element of education from the side of the consumer, no doubt. You can have, however, a policeman or a educator for that matter above everybody's head. So there is certainly an aspect of the industry training and educating the users, but certainly also a aspect of baseline security, and how do you achieve that baseline security? You achieve that

baseline security by providing security at the design. You achieve that baseline security by providing security at the point of sale.

You achieve that baseline security by providing some level of security at the network environment. In the end it's about all layered defense. It is about making sure that the consumer is your first line of defense. But at the same time, that you equip the necessary technologies and you put those in place to have redundancy in the system.

Who would like, I see, one, two, this is going to be a popular question, you want one too? Okay. Let's begin right to left. You want as well? Please.

>> YUEJIN DU: I would like to add something. I agree with what the moderator said. In addition, I think from a consumer perspective, what he can do is rather limited. What I would like to add is that there are many basic security elements that can only be forced through by governmental agencies. For example, the attacks in the United States is just this example.

The problem occurred in my device, will not affect myself but actually affect others. Security in public environments, this kind of things must rely on governments to enforce security. Everybody must do

their job to secure other people. This is what I want to add.

>> ILIAS CHANTZOS: Go ahead.

>> JAMES SNOW: That is great. I think we are all going to agree violently on different aspects of this.

I agree with what everyone is saying. But add a little bit more, I'm actually reminded of the earlier presentation from the gentleman from Deutsche Telecom. We have to make tools that are easy to use. And the other aspect is going to be bribery.

At Google, we have built in what we call safe browsing technology, because we are able to index the entire Internet every 11 minutes, we are able to detect all the different sites with malware, ransom ware, all these viruses.

What happens is if one of your users tries to go to one of those sites, either in Chrome or Firefox or safari or Mozilla, they get this big red screen of death. Maybe you have seen it in your personal life. We try and prevent infection. We need to have tools that are easy on the user. The other part is bribery. I mean that users are lazy. They are not security experts.

You need to incent them to do good security practices. For us at Google we have started a programme saying that

we will give you free terra bits, free Google drive space if you enable things like multi factor authentication and you lock down all your different devices.

So you have to use a little in English as we say a little bit of carrot and a little bit of stick.

>> ILIAS CHANTZOS: Thank you. The bribery and choice of the term as well is particularly interesting. Thomas Kremer, you want to say something?

>> THOMAS KREMER: Briefly. Referring to your example, baseline security, I want to have it, education of people, I want to have it. I want to have both, because I think if you want, if you are a effective Cybersecurity, we need the people, we need education of the people. We need that people are aware of what they are doing on the one hand. On the other hand, security by design is really necessary, and as already said, simple to use tools for security is the key.

>> I'd also like to add one aspect. Security is a matter of time also. It is a race if you like. We are racing against people who are doing their own research also. But what we see today on the Internet is that the Internet has become a sort of jungle, in which there are pirates. It's hard to localize where they are. They are often not in the same country that you are, but they

can get into your private computer, they can get information about you or about private companies.

They can hold you to ransom. They can hold government organisations to ransom. Beyond issues of security, this is a question of international law. There is also a financial issue, because if you look at what these bad guys are doing, they are not robbing banks anymore. They are attacking companies in this way.

They want to be paid in bitcoins. Bitcoins is a currency that does exist, but no individual country is responsible for governing it. All the currencies in the world, apart from Bitcoin, have a government, a state that is responsible for managing that currency. I don't quite understand why. I'm not quite sure what the reasons are for this. But some banks and organisations are happy to handle bitcoins, although the very existence of this currency makes it possible to conduct illicit acts.

My question is, why is is it the financial institutions and even governments are happy to handle bitcoins, which is a way of laundering money from these illicit actions.

>> ILIAS CHANTZOS: The money point, I think that's a good investigative technique in every case.

>> Can we have a quick show of hands to make sure

you are awake if nothing else, how many of you in this room have actually undertaken Cybersecurity training at work?

Right. We have got less than 10 percent of you. Here is the thing. Employees, they are also citizens. When they are at work, their employees. When they leave work, they are citizens.

If the industry and we are all in the industry, if we are not doing enough to train the people in the industry, how do we expect the people outside of the industry to understand Cybersecurity?

Another request for you guys. When you go home, you will go back to your organisation, and you will say, we need to start training people in our building on Cybersecurity. So protect our company, and we can by osmosis start to train the rest of the population. That is what industry can do.

Government needs to do more. It needs to do more of the basic education level and countries like Poland and Romania do have quite aggressive programmes in place to train all of their citizens on Cybersecurity in the coming years.

It is possible. It just needs effort. We need to stop talking about it and start getting on with it.

My last point before I shut up, there is a difference between compliance training and awareness. Compliance is what we do every company pretty much does it, I'm shocked that you don't. You get people in a room once a year, I shout at them for half an hour, I get them to sign a piece of paper that says I've shouted at them for half an hour and understand Cybersecurity.

That is just for the auditor and pretty much it's worthless. Then you do training which is specific to their role. If you are a sales engineer or a salesperson or support engineer, the training you get needs to be different to your role. Finally there is awareness. Frequently pushing out reminders, because you have got to keep people remembering. They have to be professional every moment of every day.

>> One minute, please.

>> To add to that, awareness is a good thing. We should go for that. But we still need regulation and a good example is again from the car industry, if you go back to the safety belt, the reason why the people are today using the safety belt is not only because of awareness. It is mainly because there is a mandatory regulation for putting that.

That is in Cybersecurity, not in a different way.

>> ILIAS CHANTZOS: Ladies and gentlemen, I'm very pleased that we are able to offer you both a discussion as well as the individual perspectives in the debate. The conclusion, I like that we conclude with a note of agreement, it is people and policy that will better drive Cybersecurity and obviously your role as standard making bodies, as regulators is equally important. Thank you very much for attending and listening so closely. Enjoy the next session. Thank you.

(applause). (pause).

>> BILEL JAMOUSSI: We are moving -- can you hear me?

So we are moving now to a session 4, standards parties approach to security, privacy and trust. Is it chaired by Toni Eid, the editor in chief of Telecom review. After the session, there will be a coffee break for about 20 minutes. During this time, we will finalize the report of this Global Standards Symposium, and then we will be back to read through that with you.

Thank you.

>> TONI EID: Thank you. In fact it's a challenge also to moderate late afternoon. Okay, so I hope everybody wakes up and can join us with the conversation.

So, recognizing the crucial role played by standards

and ensuring security, protecting privacy and establishing trust in the ICT infrastructure and services become crucial due to data increase and everything now is on-line. Highlighting the security, privacy and trust, established area of work in many international standards bodies that address ICT and other technology areas which call for standardization to address these challenges, we have a very distinguished panel today.

I will give them to start quickly, so before we start the Q and A, so and I would like that as much as we can to make it interactive, so please, okay, I know you are tired but let's do it more interactive. Now I start with Miss Karen from my right, please.

>> KAREN McCABE: Thank you. I need the slides, please.

>> TONI EID: Sorry, we start with Sophie Clivio to keep the order. Thank you.

>> SOPHIE CLIVIO: Okay, good afternoon. Just to keep you awake, my name is Sophie Clivio, I'm working for ISO. I know we are just before the coffee break and we have several presentations and maybe the subject of standardization is not that sexy. But I'll try to explain what ISO is doing in the arena of privacy, security and trust.

I will begin by some explanation what ISO is.

ISO founded in 1947, is an independent nongovernmental international organisation, with membership of 163 members.

Through its members, ISO brings together experts from all around the world, and as you can see, we have something like 100,000 experts coming from many stakeholders categories, including industry, of course, government, consumers, NGOs, academia, etcetera.

So all those experts come together to share their knowledge and develop voluntary market relevant and consensus-based international standard.

Why do I say voluntary? Well, I think it's important to mention, because we hear the questions in the sessions before, voluntary international standards because they are created only if there is a market need on a voluntary basis by the experts.

Voluntary as well, because ISO itself do not enforce the implementation of these standards, so that is the difference between the international standards and regulations. The ISO standards are implemented by the market as they wish so. Of course, some governments might decide to include reference or to copy some of the international standards as part of their regulation.

But that's their decision.

ISO in itself develops voluntary standards. Right now, we have something like 21,000 standards in the ISO portfolio, and we are publishing something like 1200 standards a year, which means 100 every month. 100 standards is not 100 new subjects. Half of those are revision of existing standards, and the rest is pure new standards.

I've lost my presentation.

So maybe let me continue without the presentation. We will see if it comes back. Yes. So, the ISO members that you can see on this map are covering all around the world. We say that we are covering 98 percent of the world GNI, more than 97 percent of the world's population, and as you can see, 75 members, 75 percent of the ISO members are coming from developing countries.

So on top of the 238 technical committees, developing the international standards, ISO has three policy development committees. One of them is called defco and I mention this committee because it's very important. The policy committee for developing country is the main goal to ensure that we have as many experts from developing countries participating in the work of those 238 technical committees.

So what is the ISO approach to security, privacy and trust? Well, the ISO mandate is very broad. It covers everything but electro technical issues covered by our sister organisation IEC.

Because it's very broad, ISO takes a multidisciplinary approach to security, privacy and trust, meaning that it's developed in several committees.

One of the policy development committee that have not yet mentioned is coPALCO, committee for consumer issues in ISO. It is very important because it's bringing the consumer views into the development of international standards, and we have seen that especially in this area the consumer views are important. It is working on several issues including consumer privacy and looking at privacy by design as well. So it is one of the committees dealing with this area. Some others are mentioned on this slide. Just to give you some of them, TC292 is the committee on security and resilience.

It is working on several issues like organisational resilience, authentic city, integrity and trust for products and documents. So many issues relating to security and privacy. We have the technical committee on risk management 262. They have developed international standards called ISO 31,000. Principle

and guidelines for risk management. Just want to mention two new committees, they are recently created. They have less than one month. Technical committee 307, electronic distributed ledger technologies so obviously, the privacy and trust will be at the cornerstone of the development of this committee.

And the other one is TC309 organisational governance.

The next one, there is appearing on the slide, and that I will describe on the next one is JTC 1. ISO, IEC JTC 1 is the committee dealing with information technology, that is jointly shared between ISO and IEC.

This committee is a very big committee, with the participation of more than 100 members. We can say that they have 500 work items on their portfolio. And they are responsible for something like 10 percent of the ISO programme of work. So very big committee, which is developing several groups, something like 20 active subgroups. I will give you some of them, present them briefly, because they are relevant to the area.

We have JTC 1SC27 dealing with information security management, including the standard that was mentioned before and just because I want to be right, this is not ISO 27001. It is ISO IEC 27001.

We have JTC 13017 dealing with biometrics working in cooperation with EK or for biometrics standards. JTC 117 card and personal identification, part of their documents are the machine readable travel documents.

SC14, IT service management and governance, why do I mention this one? Simply because of the outsourcing that happens, the business process outsourcing and including cloud computing will be, we heard of the challenges of privacy and trust and will be looked at by this technical committee. I'm asked to speed up. So I will try. Some future work to be developed in JTC 1, cyber insurance, cyber resilience, cloud computing, big data, IoT of course, privacy, with some de-identification techniques that was also mentioned this morning.

Without forgetting the new TC that I mention on block chain that will be at the cornerstone of transparency and trust. To conclude, ISO is presenting all sectors, every sector I would say, and ISO is very well-positioned to bring together communities that were not used to communicating in the past, but that have to do its with ever increasing reliance on ICT based products and services and the resulting security privacy interest that goes within.

We can work but we cannot work alone. So we do

believe in cooperation with peer organisations, IEC and ITU. We have several joint workshops to ensure that we are working in the same direction. And cooperation with key organisations, such as IEEE, EKO, Interpol but this is not exhaustive, but it is very important. ISO does support the premise that efforts should be enhanced by this collaboration but not duplicated in order to develop market and global relevant international standards in the area of privacy, security and trust.

>> TONI EID: Thank you very much. Now we give the floor to Frank from IEC as well, please. Frank.

(applause).

>> FRANS VREESWIJK: Thank you very much. May I have my slides, please?

While we wait for my slides, my name is Frans Vreeswijk, general secretary of the IEC.

A few words on the IEC, perhaps to start off with. It was founded in 1906, 110 years ago by the industry as a, like ISO fully independent organisation nongovernmental. We bring together 167 countries in our family, and some 20,000 experts. We have some 7,000 standards that are being maintained. Of course, also, like was mentioned our standards are voluntary standards. We don't enforce them. Only regulators can say that they

have to be part of the regulations and so forth and can refer to them, but in principle ours are made because there is market needs and the market demands and so forth.

Let me focus on how the IEC international standards and IEC conformity assessment systems how they can build trust.

Cybersecurity is central to the safe operations of industrial installations, critical infrastructures, and together with privacy it is absolutely key in the digitalization of for instance healthcare.

Staggering amounts of data are traveling through systems and devices, and much of it is sensitive. We heard about that today. We as IEC prepare many of the relevant horizontal standards that take into account the different security risks and needs for manufacturing plans, utilities, hospitals, or consumer electronics.

The IEC has published more than 200 security and privacy related international standards. We also have a special advisory committee on security in place, that is coordinated the work across many different technical committees.

Most of the international standards for power system management and associated information exchange are developed in ICT C57. Published standards help to define

the security of communication protocols and include end-to-end security issues.

IEC TC45 is responsible for publishing international Cybersecurity standards to ensure the safety of nuclear power plants. It also in close collaboration with the international nuclear energy agency.

The mass digitalization of industry which is collectively called often as industry 4.0 or smart manufacturing, requires a unprecedented integration of systems, all of which have increased security needs. Already today, the standardization requirements of the process and planned for are largely covered by the IEC. We have published most of the important international standards, that cover among many other things the security of networks and systems in industry, processes, controlling automation, and these international standards address both individual devices as well as the whole industrial network.

They provide metrics for assessing the security of systems as well as guidelines for the design, operation of the systems.

Healthcare. The impact of information technology on healthcare is also fast expanding. Medical care rests

a trust, trust between patients and the doctor but also increasingly medical equipment and data are safe and secure.

IEC TC 62 which prepares most international standards for medical devices has a particular focus on data security, data integrity and data privacy to protect personal data and identities of patients.

Now with the advent of health variables, new systems are needed, that oversee the sharing of health data from patients to doctors. Active assisted living or AAL as we abbreviate it is another topic that will require increased efforts with regard to privacy and security.

In a systems approach, the IEC has put in place systems committee AAL which collaborates with many different fora which are here as well as with ISO TC 215.

The IEC perform the assessment system IEC EE verifies and certifies the devices and systems used for energy generation in industrial automation, healthcare or in consumer devices that they are safe and secure. Certification is an element in the chain of trust.

All of these areas I mentioned are part of what we call the Internet of Things, IoT. The wireless sensor networks that enable data collection for big data, and

sharing in cities, buildings, transportation, manufacturing, and many of the other applications I already mentioned, they require a different approach to security. They are not traditional computing devices and relevant standards are in process in the IEC.

Incidentally, the IEC contributes to many of the technical building blocks for the IoT.

Then we come to ISO IEC JTC 1. We have a joint committee, ISO and IEC, JTC1. This focuses amongst others as indicated on Cybersecurity and privacy. I had a few words on subcommittee 27, which has its focus specifically on security techniques publishing international standards that aim to protect the information in communications. A lot is going on there, including cryptography and other security mechanisms, biometrics and identity management.

It also prepares auditing requirements, accreditation, evaluation and conformity assessment criteria in the area of information security. The IEC would like to see a broad cooperation on Cybersecurity, and privacy concerns, because all the organisations standardization organisations, none of them can do it on its own.

Here ITU cannot do it on its own. You need ISO,

need IEC, and we all three have said as all three organisations that we would like to work together.

We have demonstrated IEC more than once its collaboration standardization can definitely help to reduce duplication, waste of time and money, and to ensure better outcomes. So we call also here for awareness and for similar approach. With that, I would like to thank you for your attention. Thank you.

(applause).

>> TONI EID: Thank you, Frans. Now I propose to give the floor to Miss Karen, please.

>> KAREN McCABE: Good afternoon. I'm Karen McCabe, with the IEEE where I'm a senior directer overseeing our technology policy and international affairs.

It is such a pleasure to be here today and I want to thank on behalf of IEEE ITU and Tunisia for hosting GSS 16 and WTSA. It is an honor to be here and also to be on this panel with distinguished speakers.

The power is in the clicker.

(chuckles).

To ground my presentation I start by sharing a overview about the IEEE. As we go through the presentation, you will probably see why I want to take this approach to kick us off.

IEEE is one of the world's largest professional associations. We have 420,000 members around the world and we are in over 160 countries. It is grounded in its global membership and collection of technical societies as well as its hundreds of local sections and chapters around the world, they provide for local engagement across the globe.

It's also known for its platform of education, publications, technical conferences. We have literally one to three conference a day around the world somewhere.

It has a portfolio of initiatives that are open to all. IEEE members and nonmembers alike. They are in Cybersecurity, we are starting work in technology ethics and there are many others. It also has strength in its affinity groups such as women in engineering and many humanitarian efforts. All these initiatives work together and we are seeing a increasingly multidisciplinary engagement with those across technology and industry sectors and domains.

In addition I triple E is also a global standards developing organisation that works in collaboration with our colleagues sitting on the stage, ITU, IEC, ISO and other regional and national standards bodies.

In the standards association, which is the standards

development arm of the IEEE we are also known as the standards association, IEEE SA. We work in standardization eco system to provide quality market driven and market relevant standards environment that is respected worldwide. It represents one of the many communities of IEEE where participants are particularly focused on developing standards in a open standards development process which is rooted in inclusion and transparency. Currently we have over 1300 global standards that are active or in development. We have over 500 working groups whose participants come from around the globe developing standards. Standards span a spectrum of technologies.

Here are a few that are represented. As we are seeing, we are all discussing through the day here, we are seeing a integration in the role and impact of ICTs through all of these technical domains, and also the embedded aspects of security, privacy and trust. Everything is becoming very critical and very interrelated.

As many of us in the room know, standards are very important to the, to what we are talking about. They are a central piece of the puzzle and of the solution that is we are looking at when addressing privacy, security and trust. As we have heard today, we have seen

the theme that there is such a rapid rate of technology development, and with more people around the world coming on-line with new technologies such as IoT and devices and people being connected in unprecedented ways, ICTs are going to continue to play a critical role in reaching not only the Sustainable Development Goals but enabling technological advancement for humanity. Security, privacy and trust are, and confidence are part of that.

When developed working a set of principles for voluntary cooperation and use among all stakeholders and that represent technical excellence, enable interoperability which is critical in fostering innovation, and here we see some of the principles that IEEE along with many organisations, including those on the stage, do abide by from open direct participation, do due process. We are working to reach broad consensus. There needs to be balance, transparency, which has been another common theme we have been hearing today, universal openness, as well as coherence. We talk about coherence, we are here focusing on coordination among industry, government, associations, NGOs, other standards bodies. It is critical that we are all in this together.

As I'm mentioning, when we look at our collective

efforts to address security, privacy and trust and confidence challenges, through the lens of standardization, to notice the value and impact of open standardization processes and open standards developed through these processes, open processes are good practice from a security perspective, as more people are involved, you will have a more set of eyes on issues and more experts to help solve problems and to maybe discover potential flaws.

Transparency is also critical, is embedded in open standards development processes. That helps build trust in platforms and services and products that are going to be built or adhere to the standards. Open standards enable privacy and security enhancing technologies to gain widespread adoption, as they promote interoperability which is foundational to the challenges that we are facing today.

Open standards fuel innovation that can advance solutions to the challenges of security, privacy and trust.

As we look at the challenges that are facing us, with privacy, security and trust and confidence, progression on addressing these will take unprecedented collaboration across all stakeholders, industry sectors,

technology domains, disciplines, even generations and cultures of people.

It will require taking into consideration ethical dimensions so that we understand the impact of technology and standards from a human-centric lens or perspective. There is a need to continue the trend from vertical development to collaborative development and to bring stakeholders together to discuss synergies and overlaps, strengthen our cross sector and discipline collaborations and identify new approaches and resources to advancing solutions to challenges. When we look at the challenges from a standards perspective I'll share several recommendations. One, core functionality should be standardizes so that helps enable innovation above and below the standard. Open standards inspire innovation. To include a new generation of privacy, security and ethics professionals in our processes, among others from cross multiple disciplines and open standards development. We are seeing such a rapid rate in technical development, multidisciplinary, multi stake holder approach is so important, but it is also important to bring in a new generation of developers and technologists among others into our processes.

To build privacy, security and ethics best practices

into open standards themselves, to help contribute to trust in ICTs and our growing global digital future, can embrace a globally open inclusive paradigm that will ensure and promote interoperability and integration and synergy across the value chain globally and establish integrated standards ecosystem framework that takes into account current technologies and also future or anticipated state of technology and its impact to learn from the past on understanding what technology and its impact can bring, especially in the domains of pricey, security and trust and confidence.

In closing, and I think we have heard the theme from my colleagues on stage here, is in standards we use the term interoperability and coexistence from a technological perspective so things work together and there is economies of scale. But also from a ecosystem perspective of all the actors and stakeholders involved, it's important that we also work in interoperable way and go beyond coexistence.

I thank you so much for your time and I will conclude. Thank you.

>> TONI EID: Thank you very much.

(applause).

Now I give the floor to Mr. Ashok Ganesh.

>> ASHOK GANESH: Thank you very much. Good afternoon. I'm Ashok Ganesh from two organizations, CEN and CENELEC based in Brussels, we are two of the three European standards organisations recognized in Europe as providers of European standards.

Many of you in the room will have heard of our sister organisation, the third ESO, European standards organisation, that's the European Telecommunications Standards Institute and I'll come back to ETSI in a second, to say CENELEC and CEN are standards organisations and electro technical committees in Europe, and we have in each organisation 33 national members, and we also have a range of affiliates around the periphery of Europe. I'm pleased to say that the Tunisian standards body is affiliate of both CEN and CENELEC.

That is a good thing. To come back to ETSI, telecommunications, ICT, not long ago many of my colleagues would have said, ICT, certainly we don't do ICT, so and a little bit in CENELEC but CENELEC electro technical would be closer to the ICT world anyway. Just to therefore, my presentation is really about a journey that CEN and CENELEC are on, it's all about us basically (chuckles).

It's, despite my gray hair, I would regard myself

as one of the new kids on the block in this field. I don't know if you can suspend your incredulity for a second, all will become clear.

On this slide, this was an attempt to show even though we are European regional organisations, we have a extensive network, and that sometimes extends to global partners, but the main thing I want to say on this slide is to say that all of our CEN members are members of the ISO and all CENELEC members are members of the IEC.

We are in a privilege position because we can look up to and work with organisations global organisations like ISO and IEC and that gives our stakeholders in Europe a tremendous advantage, and I'll come on to that more in a second.

Yet ISO and IEC are big brother and big sister, if I can say that in a nonOrwellian sense. We really do work very closely with them. We really very much appreciate them.

Moving on, the colleagues from ISO and IEC were very, what is the word, modest about JTC 1. JTC 1 joint ISO IEC technical committee on IT is a incredible resource for the world. We in Europe are starting to wake up late but nevertheless we are starting to wake up as to the real, the benefit, potential benefit that is hidden in

the huge amount of work in this area, and that certainly in Europe we hope to exploit more in the very near future.

I'll move on.

This slide has been very well covered by my colleagues. Yes, voluntary nature, Sophie explained that, national delegation principles, our way of organizing all of the needs for standards in all the various sectors that we cover and that we are independent organisations, independent private organisations, not directly linked to government, but our standards in many cases can support the implementation of regulatory policies in Europe and beyond.

This slide indicates or shows one of the main points of difference in Europe through CEN CENELEC once we agreed to European standard, that standard must be published by all of the 33 countries, and any standards which existed previously that could conflict with the new standard must be withdrawn from the market. In one go in Europe, a new standard covers from Iceland in the north to Greece in the south, to from Finland to Portugal and all points in between, the same technical agreement is in place.

That is an important difference, we think an important value in Europe. Coming on to the topic at hand, this slide, sorry, the printing is a bit small,

but this is a time line. What I want to say here is, CEN CENELEC have lived a rather maybe privileged and maybe cozy relationship with our main stakeholder industry, for a number of decades. If you look back to the 1960s, '70s, '80s, everything was understandable. Everything was neat, in vertical sectors, energy, manufacturing, transport, personal protective equipment, pressure vessel, consumer products, food, aerospace, I can go on.

As we come towards the end of the 20th century, things start to get more complex. If we come into the years now 2010 to 2020, the reason we are all here today in this room is because things have become very very complex for everybody, with the advent and the take up of new technologies, new ICT technologies. That cuts across everything and it certainly cuts across the cozy relationship that CEN and CENELEC had for years with our traditional industry stakeholders.

Therefore, that is really the journey I mentioned earlier, that we are on, is how are we as standards organisations, how do we even keep up with let alone meet the needs of our traditional stakeholders, because you can bet your bottom dollar if we don't need their needs, somebody else will. To keep our relevance and

our place in the market as standards providers in Europe, we need to evolve. Let me catch up. I'm sure there are things I've forgotten getting excited.

We mentioned stakeholder in traditional sectors are getting involved with Smart Cities, e mobility, industry 4.0 being a big topic in Europe. I mentioned E mobility.

Intelligent transport system to name a few things. What the future holds on the right side is anybody's guess. We will find out when we get there.

What we recognized in CEN and CENELEC, we have a strategic challenge, that is to support the take up and use of digital technologies in traditionally nondigital sectors. As I said, we as organisations who are the providers of the platforms that standards in which standards are developed, we even apparently don't even understand the terminology. I'll give you an example in a minute.

We see a complex and urgent need, and if I show you the next slide which comes from an organisation in Europe, the alliance of Internet of Things innovation, and this is one of the analysis, you may well be familiar with this slide, I certainly wasn't, and it proverbially blew my socks off when I saw it. If you look at these

are vertical sectors, and there is a big horizontal one at the bottom, and these are all the potential bodies providing technical specifications or standards for each of those home building and automation, manufacturing, vehicle and transportation, healthcare energy cities, wearables, agro and farming.

If I find it complicated, maybe our industry partners don't find it quite so complicated. But I think it is complex. We are trying to find our way. We are appearing in many of these blots along with ISO and IEC and IEEE. That is good already. But we can't say we understand much beyond that. In the summer we had a European workshop with our industry, called digital transformation of industry. What does industry need in Europe that standardizes and CEN and CENELEC need to furnish?

The key things that came back from industry was about standards for IoT, big data, cloud, 5G, Cybersecurity. Everything is going well, because we understand those things or we know a little bit, at least we know the names. Then we started talking about block chain technology and quantum technology and we were back at square 1. ISO is ahead of us with TC 309, is it? 307. I can't read my writing.

So, things are complex. What do we see regarding privacy and security? We see that stakeholders are taking up these technologies and from, for example, Internet of things, even in that process, whether they are customer focused for products and services or internal, we see things are connected, generating data, transmitting data, storing data, analyzing data, transferring, transmitting the results of the data.

Yet there is a risk and there is something we still need to deal with. There are data silos. But somebody said earlier, you cannot do business without trust. That is one of the messages we got back from our stakeholders.

There is a need for, definitely a need for standards. That is another thing we learned. There is another thing which is perhaps, even comes before standards, all the stakeholders in this complex area, they need frames. They need frames to understand what, how legislation is moving ahead. They understand what the other standardizers are doing, what the standardization landscape is. They can talk the same language as the vertical stakeholder participants.

At the end of the day, the business needs the real standards for IoT, cyber, big data, but they also need somebody to help them navigate through this very complex

fast moving time. That is what we have learned. We aspire in CEN and CENELEC to be that frame. Coming on specifics we are working on a request in Europe from the European Commission to work on a so-called mandate, they are not called mandate any more, standardization request 530 on privacy management in the design and development and in the production and service provision processes of security technologies.

This is a very important area, as it gets to the bedrock of security by through design and thinking. We found it's difficult to get industry experts to work on very broad topics and hence the work programme is on very defined topics. Data protection, video surveillance and the last one on the list which is obscured, biometrics for access control, including face recognition.

We have to bridge that gap. That is still a challenge for us.

We also have a, what we call a focus group on Cybersecurity, and that is looking at identifying areas where standards are needed. I come back to the ISO IEC 27001, information security management standard, and that will be submitted in Europe very shortly to an adoption procedure. If the outcome is positive, that

will become a European standard as well and probably not before time.

In quarter 1 of next year, we aspire to hold a workshop on vertical needs for privacy, security. It will be labeled Cybersecurity. Just to note, it is obscured by the text box, but the last of the bullets, square bullets on the list is actually functional safety. My boss is convinced that this brings everything full circle, because this is what CEN CENELEC do. Transfers to ISO and IEC, we have many sectors for decades provided standards for functional safety. Just because we are dealing with a new field, Cybersecurity, doesn't mean to say we are not dealing with functional safety. That can help us to navigate the way forward. Thank you very much for listening to me.

>> TONI EID: Thank you.

(applause) Now I'm glad to give the floor to Dr. Reinhard Scholl from ITU.

>> REINHARD SCHOLL: Thank you very much, Toni.

Back in 2004, in our telecommunications standardization assembly in Brazil, we did not yet have a Global Standards Symposium by name.

That started only in 2008. But we had one in spirit. We had organized a one-day Cybersecurity symposium. Can

I have a show of hands, who was there at the Cybersecurity symposium in 2004?

I do see some hands. Okay. This Cybersecurity symposium, here is the flier, ended with 11 key points. These key conclusions are as valid today as they were 12 years ago. I'm citing a couple of them.

The first key conclusion was the lack of adequate security and networks in particular the Internet is very serious and becoming worse.

Another conclusion was, security must be built in, not bolt on. That means you have to put it into the system right from the very beginning.

And quoting again, this fundamental principle implies the need for a nontrivial section in all recommendations and standards, dealing with communication, architectures and protocols.

It also concluded that shareholders and stakeholders need to share information. Back then we had the first edition of what we call the ITU security manual, which is an overview of all the ITU recommendations and how to apply them that deal with security. We kept this tradition and last year we published the 6th edition so it's close to 200-page document publicly available. We recommend it for

reading.

It also concluded that there is a need for stronger international collaboration, and that standardization needs to be a viable part of the global security effort.

What has changed in those 12 years since we held the Cybersecurity symposium? For one, the scale has just gotten much, much worse, the scale of the security problem.

Four years ago, at the world conference on international telecommunications in Dubai, a group threatened to attack the ITU-T infrastructure and attack they did. We were prepared but nevertheless, we suffered an outage of perhaps maybe an hour, until our website was back up.

I'm going to tell you a couple of the problems that a small and medium enterprise has, such as the ITU Secretariat.

What do you think, how many attacks, how many cyber attacks does the ITU or is the ITU exposed to on a single day? It's more than a million.

There are five levels of severity, out of those million attacks 10,000 which are 1 percent are high or very high.

These are only the known attacks. There will surely

be also, there are also unknown attacks, and I don't know about them.

I'll tell you a couple of security problems that we have to deal with recently. Confidential information about the ITU network was leaked, and some malicious person could have brought down the network at any time. It took us less than one minute after the leakage of this information occurred to find out about it.

In a couple of weeks ago, ransom ware encrypted thousands of our files, so ransom ware is malicious software. It encrypts your files. You have to pay money and then it gets deencrypted again. We didn't pay up. We were able, because we have backups we restored most of the files but nevertheless we lost some of the files. I assume that the challenges that we at the ITU Secretariat are facing are similar to your organisation and company.

There is a very famous quote by the former CEO of Cisco, John Chambers who said last year there are only two types of companies, those who have been hacked and those who do not yet know that they have been hacked.

And with the Internet of Things, the security problem is only worsening. I just can't resist to quote one tweet that a colleague of mine sent me, that was circulating in the press, because of the attack that

was mentioned last Friday.

So professor said, quoting, in a relatively short time we have taken a system built to resist destruction of nuclear weapons, and made it vulnerable to toasters.

Another thing that has changed in the last twelve years dramatically is the amount of data mining and the mass surveillance that is permeating our society, and often a debate is characterized as being either/or. You can have security but then you can't have privacy or you can have privacy and you don't have security.

But that's probably not the correct way of phrasing the problem. You can have and you could have both, security and privacy. Mr. Edwards spoke about promoting privacy by design earlier in his speech.

Trust, it was said several times today, is fundamental to our society, trivial things like going for a pizza here involves trust. You trust the vendor, the ingredients are somewhat fresh, that no abuse is made when you pay with credit card, or if you have a pizza delivered, that no one is taking off with the pizza.

Societies with a low trust index, they waste money and resources in trying to figure out who the good and the bad guys are. There is a link between trust and economic wealth, it's not quite sure what causes what

but there is a definite link between the two of them.

Trust is also important and necessary in the ICT context, especially in today's interconnected world. One of the ITU Study Groups issued a report called, trust provisioning for future ICT infrastructures and services. One of the ideas outlined in this report is to develop a trust index so that would be a single number that combines multiple trust related indicators into one number. So similar to stock market index, which is one number which reflects the status of the markets.

An interesting question is also whether or to what extent new technologies are helping to increase trust. For a long time in human history, trust was built around very tightly knit relationships like the family or the village that you are living in. Then a couple of few hundred years ago, change happened, and all of a sudden people put trust into anonymous situations like bank and banks and insurance companies.

What we are seeing today might perhaps be yet another shift, and that is that we are starting to trust complete strangers. Can I ask again for a show of hands, who among you has been using one of these platform services like Airbnb or uber or in France, blah blah car, who has used one of those services? That is a sizable number.

That is a sizable number.

So that is just amazing. No one would have thought that this would happen on such a scale within the last few years.

I think I'm going to skip my slide on block chain which the economist label the trust machine. I'm going to come to my last slide, there is something called the world standards day, celebrated by ISO, IEC and ITU every year on the 14th of October. Every year we select a theme. The theme for this year and you can't see it because of the captioning is standards build trust. Standards and my colleagues here on the podium, have standards developed in a open, transparent and inclusive way inspire trust. One of the proposals that came to this year's assembly in the context of our resolution, Cybersecurity that reinforces inclusion, that was reached at our 2004 Cybersecurity symposium and this proposal asked that all ITU Study Groups continue to evaluate existing, new and evolving and new recommendations with respect to their robustness of design and potential for exploitation by malicious parties.

Open source will surely also play an important role and complementary role, source code that can be

scrutinized is certainly helpful and increase security.

In the future, standards may not just have maybe a security section, perhaps they also have a privacy section. There was very much interest -- I was very much interested by what Karen was saying, they are also looking into the ethical domain. So perhaps we in the future may also have an ethics section that standards will accompany.

With that, I would like to thank you and go back to you.

>> TONI EID: Thank you very much.

(applause).

Now we will take questions from the panels. Please say your name, your organisation, it's better to say to whom you address your question for the panelists, please. So any questions?

Should make the coffee break before, I guess.

Okay. I have one important question, because now really we see a lot of activity for the standardization of the security, privacy and trust. I think there is overlapping between all the standardization. So can you tell me what do you think all this, can we combine all of them in one standard? There is overlapping, there is conflicts maybe.

(chuckles).

Please.

>> SOPHIE CLIVIO: I think there is a difference between the person overlapping on standards, in fact, I would say that there is room for everyone that we need to collaborate, collaboration is the key word.

Collaboration for having standards that do not overlap in themselves. I'm not saying that the same request do not come to the three organisations, but we have ways to organise and to develop joint standards. We have many means to do that.

Collaboration to ensure that the standards are globally relevant, and will respond to the market need, it is feasible. We have several means to do it. We are already implementing that.

But maybe my --

>> TONI EID: Ashok.

>> ASHOK GANESH: Let's be clear, there are times when different standards are good, different standards are needed, and sometimes in Europe, we have very specific regulatory context, which requires that maybe the resulting standard will be different from standards in another region or another part of the world.

I think so there will always be, that shouldn't

be our starting point, that shouldn't be our deliberate end result, because nobody wins from that per se. And the ones who lose out the most are of course the users, because from industry and other organisations, and I just come back a little bit to what I said. In fact, there is this standardization layer, development of standards, standards on the market, that you can buy and use, but of course there is a knowledge layer, coordination layer, and I think standardization bodies can be better in that layer. And I certainly point the finger at my own organisations first in that regard.

>> TONI EID: Thank you.

>> I wanted to add that in the world of today we know several standardization organisations that work on similar topics. I think we can work together, I think it needs some principles. It needs actually the principle of openness, and respect.

Openness to explain to each other what you intend to do, because it's better to know that where they are from so one can stop or join the other or use one of the mechanisms that we have and one in the respect in the sense you know the organisation has knowledge in that field. And you have to bring that knowledge of that field together with the knowledge of another field to

have a optimal solution. Is it no longer isolated. We can no longer work in silos, we need to ensure permeability between organisations and groups of knowledge. For that you need to have respect. Those two principles are key for me. We can definitely work it out. And avoid the industry have to think as, if you think about the pictogram, how many there are in all those application areas, there are many, but we need to work together, and together with I triple E, ITU, CEN, CENELEC, ISO, IEC we have come together in July in the area of Smart Cities to have a first ever discussion on who is doing what exactly in this domain and what do you intend to do, and we intend to take this further to align ourselves on a voluntary basis, and I think that is the way forward. I very much support that.

>> TONI EID: Thank you. Let's hear from Karen, please.

>> KAREN McCABE: Thank you very much. I do, I echo the comments by my colleagues as well. But the other factor in standardization, to follow on the last comment, is industry engagement. We may share common values, open transparent voluntary, but there is also we do have differences in some of our processes.

I think different actors or people or organisations

are involved in standards, are utilizing those different processes as well.

With that, it's a fact that we need to acknowledge, but also that goes back into the sharing. I don't necessarily think that we have an overabundance of competition or overlap or duplication of efforts. But it's a points of recognizing what the industry needs, what the customer needs in a sense from a human-centric perspective of the people who will be using these technologies that are built or adhering to standards, and to understand that, in order to accomplish some of that, they will be using different type of processes.

>> TONI EID: Thank you.

>> More often the standards organisations talk with each other, the better. And one statistics that we often quote is, we have 10 percent of our standards is common text with ISO and IEC so that is a sizable fraction of the ITU standards. 10 percent is text that has been developed jointly with ISO and IEC. It is the identical word from the very beginning to the very end, so that I think that shows that there is a good collaboration among various standards organisations.

>> TONI EID: Thank you. I want to challenge the audience about which is more important for you, trust,

security, or privacy? Who is for privacy? When you are browsing anything on the net, who is for -- who is for security?

Trust?

Okay. So I guess most people care about security.

Who wants to tell us why you care more about security? No one wants to share his opinion for security? Okay. Thank you.

>> Believe that without security, we will not have privacy and trust, because due to the baseline for privacy and trust, thank you.

>> TONI EID: Who would like to take that? Okay.

>> I don't think the way you phrase the question is correct. You phrase it as either/or. You said who wants security, assuming if you have security, you can't have privacy or if you have privacy you can't have security. If I go to my hotel room, I can lock it. It is secure and it's also privacy, it is not an or. You can't have both. You should have both.

Now, how we can pay -- my question to the panelists, how we can give due regards to privacy considerations without the standardization development process and establish a privacy by design mind-set in the strategies we are doing.

>> Speaking for IEC of course, security and privacy are now seen as an integral part of our standardization process, in all of our technical committees.

At the same level as we say safety is. Whenever they work on say digital information communication systems or and architecture, they have to make provisions for security and privacy of the whole system. Of course, cyber threats are fundamentally different to other safety hazards. For instance, while safety concepts are based on the probability of random failure, security concepts must assume that informed actor intentionally tampers with additional system. it requires different thinking. It requires as we said by design it has to be built in. We currently have as I said in my presentation more than 200 Cybersecurity standards.

I think in quite a lot this has taken into account, and as mentioned throughout this conference, doing it by design, making sure it is proper from the start is built in, not bolted on, twelve years ago the recommendation was there already, that is what we have to do. Thank you.

>> TONI EID: Karen, would you care to elaborate?

>> KAREN McCABE: Surely. Is it a matter of education and awareness. We have come a long way, especially in

light of the challenges and the discussions around them, in various communities. But from standards ecosystem perspective and people developing standards, we have great minds coming together with technical solutions and standardizing on things. So we have interoperability. We have coexistence.

I do think it's also a mind-set, in addition to technical aspects of things, is to raise that awareness that when we are working in standards and standardizing certain solutions and technologies, that privacy, security, are sort of front and center in those considerations, when we are working on developing standards.

>> TONI EID: Ashok, please.

>> ASHOK GANESH: I think that is a really, it's tough. I think our experience with other topics which could be regarded as horizontal for standardization environment choose accessibility eco design, if you try to enforce it and say, look, you experts dealing on standards you have to think about eco design, that doesn't work. We have to be cleverer about leveraging the natural concerns and the natural interests and the natural needs of the stakeholders, and this area of privacy, trust and security, I think it's there. It is clearly obvious

from today.

But we certainly in CEN and CENELEC need to work on building it in so it becomes natural, because if we try to bolt it on, it doesn't work. It eventually gets forgotten.

>> SOPHIE CLIVIO: On the ISO side we also believe that privacy considerations should be taken into account at all stages of the standards development process. A bit more than that, we do believe that standards addressing security technologies should include data protection requirements, and standards on technology or management systems standards, that is very important. So it's the either and or that should be taken at the same time.

>> TONI EID: Thank you. Now my question regarding the open software addressing challenge, you have mentioned this in presentation. Can you elaborate more about the challenge created about the open source software?

>> REINHARD SCHOLL: I think all the standards organisations and forums are contemplating how to work with the or how the interface with the open source community.

I think both standards and open sources

complementary standards are developed in an open process, should be inclusive, various characteristics that standards should have and that is a good thing to ensure security and privacy and open source similarly can only help make systems more secure, because the code is able to get scrutinized by not just the company that makes it but by other people, so that is definitely helping to make the world a better place.

I would say the open source and the standards communities are complementary in ITU. We have taken the bottom up approach, if our Study Groups would like to interface with the open source community they are free to do so.

We will see how this develops over time.

>> TONI EID: Thank you. Karen, you want to elaborate more about the open source software challenges?

>> KAREN McCABE: Sure. Open source has been around for many years. Industry has been engaged in that for a long time.

As Reinhard has mentioned there are a lot of similar characteristics in, from sort of a values perspective of collaboration, sharing of information, innovation, regarding open source as well as in standards and traditional technical standards development.

But I think we do see and we probably should expect continued rise in open source projects, and commercialization from corporations, so in that context, I do think that we do as standards bodies need to explore the interplay, if you will, or interaction, the relationship between open source and standards, and I do think that hopefully we get to a point where it is a strong collaboration and it sort of makes open source stronger and it makes our standards stronger.

But it is a matter of looking at our respective processes and what we need to do to enable that type of collaboration and inclusiveness.

>> TONI EID: Thank you. Before we close the session, we will check if any question from the audience. So no questions. Question here, please. Can you have the mic?

>> Thank you so much. This is Ram from Egypt.

I believe the issue of trust can be addressed if we manage somehow to ensure compliance with standards, compliance with specific implementations. End users could potentially trust a certain technology if they, for example, have some assurances that specific implementations are compliant with the standard that they can understand or that they are sure that it is from the technical perspective meets the privacy and

security and safety concerns.

So, I wonder if our dear colleagues from the panelists would share some light on that topic. Thank you.

>> I think you are absolutely right with your question. It means that if you have a standard and if you have somehow a guarantee that it is implemented in the right way that you will build trust. So in the IEC we have one pillar is a conformity assessment where we check, introduce third party conformity assessment and certification, where the checking of whether the standard is rightly implemented is the subject for that third party, a test laboratory or certification body can give a certificate and to prove that.

Therefore, also with Cybersecurity, as I said in my speech, in the system of IEC EE, we have taken Cybersecurity as a subject there to work on that, and to this goal and to this end, to ensure that if there are certificates, assess it all around the world in the same way, and those certificates are there, that people indeed have more trust in the system and in implementation. Thank you.

>> TONI EID: Now we go to close the session. Thank you very much. Thank you for our distinguished panelists.

Thank you.

Okay.

(applause).

The conference will resume after 20 minutes. Now we have coffee break. So after 20 minutes, we will be here again. Thank you.

(break).

(standing by).

>> So we are ready to start the conclusion session.

Chaired by the Chair of the conference.

>> MONGI MARZOUG: So, we will start our last session to, in fact to present you the conclusion of our day's work. We will focus mainly on conclusion and as you have already received in the morning, I think, the conclusion report, and we have some modification on the section 3.1.

So we will start with this one, and if we have some remarks on other points, we will raise them.

Okay. Do you need that I read the conclusion of 3.1? So GSS participants agreed to leverage international frameworks that contain basic principles for security, privacy and trust. And establish mechanisms of implementing these principles, second, promote advance to privacy by design principles, privacy

impact assessment and development of privacy enhancing technologies. Technologies that when integrated in ICT infrastructure and services minimize the processing of personally identifiable information. Third, agreed to establish means for the sharing of information between the public and private sectors on threats to ICT infrastructure and services, best practice and mitigation strategies.

Fourth, mobilize the international community and establish partnerships to develop national capabilities to prepare for cyber attacks, increasing countries' capacity to detect security incidents and effect coordinated response to such incidents.

Create a balance between the -- sorry -- between the need to protect the privacy of individuals and encourage the innovation user of data to drive the digital economy, when designed into new technologies and services, good privacy and security practice become attractive selling points to customers and make a contribution to the improvement of the world network.

Contribute to international standards to address global issues, recognizing that cyber attacks do not respect national borders, and that breaches of privacy and security undermine trust in ICT, and that security

frameworks standardized at the international level are necessary to provide the assurance that a service's security attributes can be trusted and that a user's security and privacy needs are protected across borders.

Agreed also to promote the development of standards for de-identification of personal data and data portability, standards able to contribute to greater consumer protection and greater choice with respect to consumers' ability to subscribe and unsubscribe from ICT service.

That's all. Any comments or remarks?

Russia, please.

>> RUSSIAN FEDERATION: Thank you, Chair. Thank you very much for this document. We studied it very carefully. We fully agree with the content.

However, we do have a number of editorial amendments, 3.2, that is in 3.2 in the first bullet, or the first sub point. The verb "adopt" is used. In our opinion, such a word should not be used in a document of this symposium, because we do not take any legally significant decisions. Perhaps adopt should be replaced with support.

In 3.3, there is a similar instance, in the first subpoint, the word "adopt" is also used. We would propose

that the verb adopt here is also replaced with support. Thank you, Chair.

>> MONGI MARZOUG: Thank you. We agree on that? (pause).

Any objection on those proposals? So we change "adopt" to "support" by "to support."

Any other comments, remarks?

We agree to change to support. Any other comments on this 3.2 section?

>> For the UK, we haven't had a chance to look in depth at all of these elements. But a couple of observations strike us. For example, the UDHR does not actually establish a right to privacy. It is a U.N. GA resolution, which does not have binding effect, to the extent that privacy is in any treaty framework, you could perhaps reference the ICC PR but again, that is a quite technical area. So I'm not sure that you really want to try and characterize the relevant articles of that in so emphatic a term as are referenced.

On a couple of the other points, minimizing the process of personally identifiable information isn't really the objective I think in that clause. I think what you are looking at is to prevent unauthorized disclosure of personal information, or unauthorized

capturing of personal information, not so much processing of it.

As to contributing to international standards to address global issues, that we feel is a very broad objective. I'm sure all of the member states and Sector Members participate in standards for various purposes, but addressing global issues in general in this text is probably a bit ambitious.

We also are not quite sure what the de-identification of personal data is intended to mean. Are you trying to suggest that personal data should be anonymized? If so, there are a number of studies which suggest that is at best extremely difficult to do at all, that it's quite easy to re-identify someone you have tried to de-identify as it were.

So I think that this document is quite ambitious in its scope. It will be rather difficult to get to something that is both generally agreeable and in all cases factually accurate, especially on issues of such import where such large terms like global issues are used.

Thank you.

>> MONGI MARZOUG: Any comment on that? USA, please.

>> UNITED STATES OF AMERICA: Thank you, Mr. Chairman

and good afternoon, colleagues. We similarly note in this report that there is a lot of information that we have not fully been able to digest.

We echo the statements of our colleague from the UK that there are perhaps certain language related to global issues and standardization that it's a little bit difficult right now to say that we endorse the report as a whole.

Perhaps a way forward for the report, because we do think that it did a very good job of capturing what was discussed today, might be instead of saying that GSS participants agreed to, instead we could say, GSS panelists and discussants recommend or something along those lines, so to establish that this is a summary of those discussions that took place today but not necessarily that everyone that was present in the room agrees to them and endorses them.

Thank you very much.

>> MONGI MARZOUG: Thank you. Any other comment? Yes, please.

>> Thank you, Mr. Chair. Egypt, in principle, we support the report. However, I just need to understand which particular references, which particular phrases is problematic for our dear colleagues from the UK and

United States. That we could work upon that, and finalize a report as soon as possible. Thank you. Because it's not clear which particular text needs to be changed, and if it needs to be changed, what is a proposed new text to be added in the report.

Thank you.

>> MONGI MARZOUG: Thank you. U.S. or UK, please, which part of report.

>> UK: Thank you, Chair and thank you to our colleague from Egypt for his query.

The points that I raised that we raised are examples of several and I think if we looked at this in detail, we would find several more areas like this, which leads me to suggest that with the time remaining, we are not probably not going to be able to go through extensive changes in the room as we are and perhaps the suggestion of the U.S. would be a good compromise. Thank you.

>> MONGI MARZOUG: Thank you. If I assume the purpose of the U.S. is to change participants agreed on by speakers and panelists recommend, this is your proposal? Any objection on that? Please. Saudi Arabia.

>> Thank you, Chair. Good afternoon to everybody.

I think that if we are to achieve a consensus, and we want a consensus, that is why we are here at the GSS

perhaps those at the GSS recommend what follows or at least they have agreed upon what follows, if we put it that way, we wouldn't refer to the participants or members of the panel. Normally, it's the participants as a whole who make these recommendations.

So we would substitute agreed, agreed with, by recommends. Thank you.

>> MONGI MARZOUG: Thank you. Any other comment? Jordan, please.

>> Thank you, Chair. I think that this is an issue which should not trigger such protracted debate. It seems to me that we should be trying, we should be inspiring the right kind of debate, I support the delegate of the Saudi Arabia, I think the suggestion of the United States is a little bit unusual, if we compare this with the previous report particularly, because it is indeed the participants who recommend. Thank you.

>> MONGI MARZOUG: Thank you. Russia, please.

>> RUSSIAN FEDERATION: Thank you, Chair. We would like to offer based on the previous discussion a compromise solution. We may notice that section 3 itself is called, main conclusions. So if this is the main conclusions, then perhaps the appropriate formula would be GSS participants concluded, or participants came to

the conclusion that, instead of agreed to, GSS participants concluded.

The same thing concerns 3.2 and is applicable to 3.3 as well. Perhaps this could be an acceptable compromise solution for everyone. In 3.1 also we just noticed 3.1.4 that is the fourth bullet, if you could show us that, 3.1, fourth bullet, to prepare for cyber attacks, it's as if we are preparing to conduct cyber attacks, in actual fact most likely that is not what we are doing. I hope at least that we are trying to deflect cyber attacks at least. So perhaps to protect from cyber attacks, to protect from cyber attacks. This appears to us to be more correct. Thank you.

One more point. And also, if I may, I'd like to go back to my previous suggestion. It seems to me that the person editing the text perhaps did not correctly hear that I said that under 3.3, we also request the verb, adopt, to be replaced by support. That is in 3.3, oh, I'm told it has already been corrected. Thank you.

>> Thank you, Chair. And good evening to everyone. Chair, we share the viewpoints of Saudi Arabia, Jordan and Russia in as much as they offer a solution to this problem and as regards the proposal of the United States of America, it seems to us that it is unusual that stands

out from our tradition as was noted by the representative of Jordan. Moreover, we ourselves, we have accumulated other comments to be made. But after the suggestion by Russia, we would quite simply to say that we are in agreement with that suggestion. Thank you.

>> MONGI MARZOUG: Thank you.

(language other than English).

>> Yes, my apologies. We missed the Russian interpretation but it's all back now and everything is fine, thank you.

>> MONGI MARZOUG: Canada, please.

>> CANADA: Thank you very much, Mr. Chairman. After listening to all the delegates express opinions, I mainly realize that I was a participant, I am a participant in this workshop, I hear a number of respondents giving views about different topics on trust, Cybersecurity and privacy. I will say the quality was excellent. I might disagree with them, I might agree with them, did I not agree with the conclusions of the participants.

I didn't conclude either the conclusions were the conclusions of the presenters.

I am a bit confused when the text provided suggested that we agreed or we conclude. I would suggest that a

better approach would be that we participated in a workshop. It was, information was presented to us, and we appreciate it.

I don't know why I can tell you I conclude, I conclude one thing, it was very interesting but important topic but it doesn't mean necessarily I will agree with the statements provided in the report.

So there is balance that we have to make between the different number of delegates, some of them said to agree, another one said no, it should only be a reflection of the response so Mr. Chairman I don't think we are in a position to support any agreement or recommendation at this point in time. Thank you.

>> MONGI MARZOUG: Thank you. Any other comment?

In fact, would I like to ask United States and UK if they agree on Russia proposals. UK. Please.

>> UK: Mr. Chairman, aside from that point, there is also the additional statement of fact about the nature of the right to privacy, in the immediately preceding paragraph which is just factually not actually true.

So, while I think that the proposal of the Russian Federation is attractive in certain ways, I'm afraid that if we look closely at this text we are going to find some other things where if we look closely, we will

not, we will find other issues, where there will be questions of factual accuracy or simply the way in which information is presented that will be difficult.

So caveating carefully the nature of this document, in a way that is mutually acceptable, I think is important. Thanks.

>> MONGI MARZOUG: Thank you.

United States, please.

>> UNITED STATES OF AMERICA: Thank you, Chairman. We agree that the Russian proposal does offer an attractive way forward. However, and we have no problem calling this report the conclusions of the third Global Standards Symposium, but given that there really was not time to discuss these conclusions at length, and as I understand it, the conclusions were made up of inputs and review by the panelists and by the speakers, it seems to me that the most accurate representation of what this document is, is to refer to the, is to either refer to the panelists, or just to say, not to reflect all together that G, to mention GSS participants. I think that perhaps if we eliminate that line, and just list these things that were the conclusions of the symposium without saying who concluded them or recommended them or adopted them, perhaps that would help us just get to an accurate

representation of what this document is. Thank you. UK, please.

>> UK: Thank you, Mr. Chairman. Hopefully this will be helpful but is it possible to say instead of concluded, noted proposals to, to indicate that what follows are a list of proposals that were made by various speakers and participants. But to not characterize what this body as a whole necessarily endorses or will do with those. Noted proposals to would be the suggestion.

>> MONGI MARZOUG: Thank you. Any comment on this proposal. Egypt, please.

>> Egypt: Thank you. Well, I guess we are a little bit deviating out of the core essence of that particular document. I have a question, if I may, to the audience in this room. If I may, if you permit me. Does anyone disagree on leveraging international frameworks that contain basic principles of security, privacy and trust and establishing mechanisms of implementing these principles? These are very generic statements. Does anyone disagree of promoting adoption of privacy enhancing technologies? Disagree with sharing of means of information between public and private sectors. Who would disagree to that? Does anyone disagree on creating a balance between the need to protect the privacy of

the individuals and encourage at the same time the innovation, use of data to drive the digital economy, who would disagree to that?

So in principle, I don't know, unless we need to see something very clearly which principle or which aspect is any one of our dear colleagues feels a little bit concerned at, because to me, and I guess to many of the colleagues in this room also, these are mainly very generic, I mean mitigates the risks posed by IoT botnets so we should not mitigate those types of risks and we should not reflect that in the report after hearing very interesting and very important information from our top experts in that particular GSS event? So we should not reflect that? Thank you.

>> MONGI MARZOUG: Thank you.

>> Thank you, Mr. Chairman. Carefully listening of this discussions now, I believe participants sure of this, this essence part of this important subject, but take into account of this, some of this global sense, so let me try to propose this GSS, my proposal is, try to find those middle ground with my English, GSS strives to rather than all this concluded or, let me propose GSS tries to of those following issues. Recognize importance, we need something to do, but understand

current problems to practically carry out this quite ambitious goals, take into account of this, but we have to recognize this GSS important moment to initiate some actions. Not necessarily to agree everything but we have to indicate some of actions and stress those following items. That is my proposal. Hopefully this will be to raise above the difficult situation. Thank you.

>> MONGI MARZOUG: Thank you. Any objection on Mr. Lee's proposal to change agreed by stress the importance of.

>> Chair's microphone, please?

>> MONGI MARZOUG: Everybody agreed on that. So we change agreed by, stress the importance of, stressed to.

(applause).

Any other comment on other topic or issue or section? Thank you.

Any comment?

We declare this session is closed. Thank you very much for your contribution and participation.

(applause).

(end of session at 1800)

Services Provided By:
Caption First, Inc.
P.O. Box 3066
Monument, CO 80132

800-825-5234
www.captionfirst.com ***
This text is being provided in a realtime format.
Communication Access Realtime Translation (CART) or captioning are provided in order to facilitate communication accessibility and may not be a totally verbatim record of the proceedings.
***