ST. PETERSBURG INTERNATIONAL ECONOMIC FORUM

JUNE 16–18, 2011

PRIVACY: A THING OF THE PAST?

Expanding Technology Horizons

JUNE 17, 2011 — 14:00–15:15, Pavilion 5, Conference Hall 5.1

St. Petersburg, Russia

2011

The increasing incidence of private data finding its way onto the Internet threatens the way individuals, governments, and companies go about their business. Is this a serious cause for concern?

Moderator:

Tina Kandelaki, TV anchor

Panelists:

Elizabeth Buse, Group President, International, Visa Inc.

Andrei Dubovskov, President, Chief Executive Officer, MTS Group

Orit Gadiesh, Chairman, Bain & Company

Peter T. Grauer, Chairman, Bloomberg L.P.

Natalya Kasperskaya, Chairwoman of the Board of Directors, Kaspersky Lab; General Director, InfoWatch

Igor Shchegolev, Minister of Communications and Mass Media of the Russian Federation

T. Kandelaki:

Good afternoon, ladies and gentlemen. I am pleased to welcome you all here and thank you for coming to our panel discussion. Although everyone was saying yesterday that the weather in St. Petersburg would be bad, I arrived today, and the weather is good. I think that everyone is in a good mood, as well. Nevertheless, the discussion will be on a very serious topic. I am really counting on you, and hope that all members of the panel will have something to say. Each of you will want to ask a question and receive an answer today from the people who are the some of the most knowledgeable in the field we are discussing. It is wonderful that, thanks once again to the St. Petersburg International Economic Forum, each of you will have the chance to receive a more thorough, more competent, more professional response to questions that concern you with respect to information security.

Now, if you do not mind, I will begin.

T. Kandelaki:

I am delighted to welcome you to the discussion panel here at the St. Petersburg International Economic Forum. As a public figure and key presenter, I am particularly interested in the topic of our discussion, privacy. Like many other global topics of the Forum, it affects every single one of us. The very first time you type your name, your telephone number, or your address somewhere on the Internet, you lose your freedom and independence forever.

Most of us have already done this. I think that we have bought books through Amazon, so someone can at least see all your purchases throughout the year. If you leave your CV on Headhunter or LinkedIn, then a stranger might know more about you than your spouse does: your skills, your job, even the details of your salary. Actually, I do not want to know if somebody knows the details of my salary.

O. Gadiesh:

Especially not your husband, right?

T. Kandelaki:

But I am divorced; that is the problem. We are also sensitive about our freedom all the time, but most of us have not noticed that we lost it a long time ago; or did we? Is this true or just modern-day paranoia? We have a very interesting expert panel with us here today. Unfortunately, Julian Assange could not be with us. It is a shame, as I am sure he would have had a few things to say. However, joining us today are the following:

Elizabeth Buse, Visa's Group President for Asian-Pacific, Central Europe, Middle East, and Africa.

Andrei Dubovskov, President of MTS.

Orit Gadiesh, Chairman, Bain & Co.

Peter Grauer, Chairman, Bloomberg.

Natalya Kasperskaya, Chair of the Board of Directors, Kaspersky Lab and General Director of InfoWatch.

And Igor Shchegolev, Minister of Communications and Mass Media of the Russian Federation.

And my first question is for Orit Gadiesh. We agree that technology and the Internet have revolutionized our lives, but maybe it has taken something away too. So, do you think that privacy is the price we have to pay? Is it a thing of the past?

O. Gadiesh:

Спасибо. I am actually surrounded by people who have really modern technology. I am using the old-fashioned stuff, so I apologize.

I. Shchegolev:

It is more secure that way.

O. Gadiesh:

Precisely. Which moves us right into the issue of privacy.

You can be hacked. You cannot hack this from me. You asked if privacy is a thing of the past. I would say not yet. Is there a serious cause for concern? Yes. How important is it? I will let you be the judge. It is said that ever since democracies were created, a balance had to be struck between individual freedom and the power of the majority.

This led to certain principles and laws that protect that balance, which is quite important to most of us. The right to privacy is a classic example, and that is really what we are talking about today. Now, none of us want to live in a glass house. We also understand the government's need to know certain private things in the public interest, or for safety. Yet just the fact that something may be interesting to others does not mean that it is in the public interest by definition.

That is why authorities in many countries need to get a special court order to listen to your phones or to do any kind of search. I would say that in democracy, it has taken several hundred years to reach this point. So we are taking about a very important principle.

This room is really not soundproof. Talk about hacking. It is an important principle, and technology now is threatening that principle. What we should not do is change the principle by accident just because somehow privacy can be circumvented more than before. Let me quickly highlight three key ways the Internet is threatening privacy.

The first: Benjamin Franklin once said that three people can keep a secret as long as two of them are dead. Our problem today is that one of those people or parties is likely to be the Internet. It does not die, it never forgets, and it is always accessible.

The second thing is that the Internet also makes information almost effortless to find because it aggregates and it sorts data, which previously was literally impossible to do. Think about health records, think about purchasing patterns that you mentioned.

The third is that, unlike a piece of paper that needed to be physically found, copied, and taken away, information on the Internet is infinitely more portable. It is therefore more vulnerable. So in short, the Internet facilitates what I would call leaking.

Whether it is inadvertent, spilling of sensitive data like customer lists of credit cards when a company really does not notice that it inadvertently did it, or private entities seeking to mine inferences about individuals from online sources, things like Facebook, Apple, Google, or outright invasion—such as hacking into company files just in the last couple of weeks: Sony, Citibank, Chase, Google, and the list goes on; and I think we have all read about it; it is a daily thing—or such as nations monitoring mobile phone calls and Internet information under the guise of national security, or entities stealing other entities' information, think WikiLeaks and the U.S. State Department.

The traditional leak has really become a flood. Now, such instantaneous worldwide revelations were impossible just a few years ago, and all of this is a function of several key trends. I will mention three, and then the implications and stop there, and let other people answer the question.

First, the time we spend online and the increasing trail of information we leave behind. For example, those of you—and I bet it is almost everybody here —with a computer, a BlackBerry, and iPad, are connected for three machine hours every 60 minutes. Rather frightening at least to me, the average person's network a day—the number of machine hours that someone is connected—now lasts 36 hours. It is projected to rise to 48 hours in two years. Think about the amount of data. And by the way, you wake up in the morning, you have to deal with it too, but that is a different thing. Then there is the speed of data transmission and the number of channels over which it can pass. And finally, there is the growing number of people and institutions that are online.

According to some estimates, by the year 2020, the data that is going to go over the Internet is going to grow by 40 times. So, think about the incredible amount of data that it produces. And it stays forever, and it will be accessible forever. This avalanche has implications for business, for governments, for an individual, for society as a whole.

Now most public discourse—and it was mentioned this morning as well when the President talked—is about the huge value that comes out of the Internet. It is measured in efficiency, in increased productivity, increased speed, ability to interact with many people, all of which are true—and by the way, I do believe that in Russia, President Medvedev has done a lot to encourage it—but less is said about the flip side of that.

For example, individuals mostly use the Internet, see the Internet as positive. So, they catch up on Facebook. Few worry much or are even aware of the potential threats to their reputation until it hits them directly, as it has started to hit some people directly, and as it will continue to, even if you try to get off it. People are increasingly purchasing online, but you cannot pay with anonymous cash. Cash is anonymous. Your name is not associated with that. Your credit card information and shopping patterns are everywhere. Or it is now easy to find communities of people who share interests and beliefs. That's great. But that also means that often they stop listening to or stop interacting with those who do not, except when they wish to find them to insult them or to terrorize them.

Can all of this be handled by new legislation? Yes, in theory. But conflicting agendas must be resolved, and they rarely are. Governments, for example, played both ways, in the US and Europe and other legislative bodies, laws are being developed, and legislation is trying to be formed. But the reality is that governments still want your information, and they use it increasingly for security reasons.

So as long as that happens, the government actually is playing both roles. In real totalitarian regimes, we have all seen, it actually goes beyond that, and people actually ban any of the media channels that come in. Private entities are also of two minds. They champion protection of uses and promise them control over their data, but they are also finding profitable ways to provide access to their users’ data to third parties, often without the person's awareness.

Now, I believe that we are going to see people use it all the time. We are going to see more and more technologies that are built to protect us from those kinds of things, but in reality, we will also see technologies that find ways to circumvent those technologies, and that has been actually the kind of seesaw we have seen before.

I do not have the answer. I would say that in fact it appears that nobody does. At the recent eG8 in Paris, exactly those conflicting issues were debated a lot, and I will close by what President Nicolas Sarkozy summarized when he talked to Internet developers and he basically talked about those democratic principles that I started with.

This is a quote from him to the Internet developers: "The world you represent is not a parallel universe where legal and moral rules, and more generally, all the basic rules that govern society and democratic countries, do not apply". Now, I could not agree more. So, is privacy a thing of the past? As I said, not yet. Is there a serious cause for concern? If you care about privacy, I think so. Спасибо.

T. Kandelaki:

We have a perfect example in front of us, where technology overtakes the education system and it is impossible not to make use of it. We talked a lot today before the panel about how to prevent children from using this technology. Children understand what it is and understand that it has to be used. And I have to say that it was a real discovery for me personally to find out what books children are reading. It is, after all, the summer holidays now, and many, I would think, are keeping an eye on this. In our childhood, to read *War and Peace* over the summer was a real feat. Today, it has been reliably proven that, in four days, a person consumes exactly the same amount of information as is contained in *War and Peace*. That volume of information will continue to increase. And the number of technologies enabling you, on one hand, to digest this information and, on the other hand, to use it—for the good of some, but not of others—will also be constantly be growing and accelerating. But here, if you permit, I will continue with our panel.

I would like to ask my next questions of both Igor Shchegolev and Andrei Dubovskov. Since the Internet has no borders, does it really make sense to have regulations in just one country, for example, Russia? And isn't it true that most modern international agreements don't actually work?

I. Shchegolev:

I guess I will begin and Andrei will come in later.

Of course, there have been attempts to regulate the Internet in certain countries, which in itself seems rather strange, because we are dealing with entities which originated in an entirely different country. But since the Internet arrived, it has turned into a huge global resource, influencing policy, people's social lives, the economy, and technology... It is difficult to imagine contemporary civilization without this resource. However, it is not centrally managed. And the structure itself is made in such a way as to be unsinkable, indestructible and self-healing. The information stored there is there forever and, consequently, the abuses committed using this tool also have far-reaching consequences. This is true whether they are deliberate cases of sabotage or just innocent pranks which go on to paralyse entire sectors of the economy and sometimes even entire countries.

The question of whether the Internet can be regulated in a given country is really a rhetorical one. You close some resource and it immediately migrates to countries without any such prohibition and continues to operate from there. People who know what they are doing will always be able to bypass any filters or attempts at censorship. That is why, in our view, national prohibitive regulation is absolutely useless: it runs contrary to the very essence of this technology and, to a large extent, to the public mood.

Another problem is this: are there crimes and offences that the government should tackle? Of course there are. And, to a large extent, offences committed on a national scale can be dealt with using legal instruments that already exist. After all, the Internet is only a conduit. And the offences committed on the Internet are indeed crimes, just as if they took place on the street. If someone snatches your purse on the street, it is a crime, just as it is if someone steals your information and uses it to steal money from your account. And you can fight it here, if these offences were committed within your country. If they are committed abroad, it is a far more difficult task, and will remain so until the representatives of various states sit down and agree how to counter them.

One such attempt has been made. It is what is known as the Budapest Convention of the Council of Europe, which, among other things, allowed action to be taken to find and prosecute online criminals in foreign territory without giving prior warning to the authorities of that country. It is largely because of this that the Convention did not work. Many countries, including Russia, considered it impossible to ratify it. And Russia, in particular, raises the issue that we need common rules to combat what are clearly crimes, which would be considered as such in any civilization and every culture, in any nation. We need to come to an agreement. However, there is no such consensus as yet, although we believe that a platform where this could be achieved already exists. By which I mean the International Telecommunication Union—the oldest international organization, twice as old as the United Nations.

We need to agree on basic principles, to say that this or that behaviour is absolutely wrong, everyone agrees, and we must do all we can to combat this scourge. We believe that this can be done using the example of child pornography, because there is no culture where it is permissible. And we are actively seeking allies around the world to support our approach.

Of course, one of the most important issues to consider when trying to solve this problem is private life: the information held on the Internet about individuals. It is a question of how to deal with that. There is another side to this, which is the anonymity of the Internet: most of the Internet is, after all, still anonymous. To a large extent, this can be exploited, but, on the other hand, it protects many people who share information on the Internet, or search for this information. So, there are two sides here and we always have to seek a balance.

In answer to your question, I would say that a single country cannot effectively resist all of the offences that are possible on the Internet. We see no point in introducing prohibitive laws on online activities at the national level, but believe that coordination is needed at the international level. We need common rules of the game, which would correspond, above all, to users' and citizens' interests.

T. Kandelaki:

Before Andrei continues this discussion, I would like to ask you something, Igor. You are surely aware of the conflict around the blogger Matviyenko, who turned out to be a man in the end. Our esteemed media and many publications printed excerpts from this blog, and it became a topic of debate throughout the world press. Do you think, in this case, that this could have been prevented somehow, that this person could have been checked out? After all, in a way, he, too, caused some harm to the entire country.

I. Shchegolev:

Each society must decide for itself which is the more important—anonymity or transparency. And it is impossible to give a clear answer here. This is a matter for public debate, a question of creating this environment. It is a matter of balancing the interests of the citizen and society. And I believe that discussions such as ours contribute to finding that balance.

T. Kandelaki:

Andrei, the floor is yours.

A. Dubovskov:

At one of the previous open forums, which took place not long ago—I mean the Sviaz-Expocomm exhibition held in Moscow this May—the honourable minister and I disagreed on one issue. So, having attentively listened to Mr. Shchegolev just now, I am pleased to inform you that the balance will be restored. I am certainly willing to support his position, but at the same time would like to draw your attention to the formulation of the question itself. You see, it is not a question of whether there is any sense in cross-border regulation, or whether each country should confine itself to its borders. Confinement within borders is the default position. That always happens when new technologies and new capacities arise. The state always tries to adapt its available resources to these new capacities. This is a normal process. We cannot say that it is right or wrong. That is how it always happens. Their own national, mental, and other priorities—including, of course, the most important among them, sovereignty in security matters—is another matter, and we should be able to enter all of this initial data into some sort of cross-border agreement. We must reach an agreement that will satisfy all parties concerned. Yes, there have been failures, for example, with the Budapest Convention, but again, this is to be expected. This is just the first step towards the creation of a supranational system, governing relations between the individual and society in the online sphere. I will leave it at that, thank you.

T. Kandelaki:

You know, I cannot help but ask, because we are talking a lot about private space and its protection: have you signed up to any social networks? Do you use them at all? Or, as someone who understands what the consequences of this can be, are you protecting yourself by not registering anywhere, or by registering under another name?

A. Dubovskov:
Welcome. I very rarely use social networks and, indeed, am registered on one of them. That was a long time ago, when it had just appeared. However, as it stands, I have not done anything new on there for several years.

T. Kandelaki:
You mean on that social network, right?

A. Dubovskov:
Yes.

T. Kandelaki:
So it all went well for you?

A. Dubovskov:
You know, I think that when starting a discussion on such a serious topic, it would be best to turn to some kind of statistical data. Now, I, for example, have no information on the percentage of people who have experienced actual harm from this lack of regulation. That is one side of it. On the other hand, it would be interesting to have some market research on the subject, to be able to understand how significant the problem is. So it is, let us say, something of a dilemma: everything is stored there forever and can have an unwanted impact on your life. That much is clear. So this dilemma exists. But how significant is it?

You know, there are a great many dilemmas in the world. It would be very interesting to get some data based on market research. What do people see as a problem, on one hand, and, on the other hand, for how many people has this really been a problem? For some reason, I suspect that a vast number of people will see this as a problem, but that the percentage of people actually affected would be no more than the percentage of people for whom the problem involved crimes outside the virtual space... or at least, it would be within the boundaries of statistical error... maybe I am wrong. However, it seems to me that, for the purposes of our discussion, that kind of information would be of interest.

T. Kandelaki:

Thank you very much. I think you are absolutely right. Moreover, if one of the panellists is able to provide clear examples, it would be very informative. Everybody knows perfectly well that Julian Assange himself began as a hacker who, if I remember correctly, was invited, after a suspended sentence, to work for a bank security department. And this switch, which also raises many questions, is, in a sense, an example of what you are talking about. It would be nice to hear, from both the participants and from the audience, some examples of what really concerns us. Has anyone ever personally run up against the issue of the dissemination of his or her personal information, submitted during registration on a network?

Natalya Kasperskaya, my next question is for you. We have just discussed the regulations "from the state’s point of view". As someone who develops software, can you tell us the truth: does the state, the regulator, possess enough tools—I mean the technology and software—to regulate the Internet? We cannot permit them to protect us, but I am very interested: can they really do this?

N. Kasperskaya:

Yes, I understand the question. On the one hand, theoretically, I must, of course, agree with the Minister, that regulation through prohibition is pointless. On the other hand, when we speak about security in general, we should not lump everything together. We are starting to talk about this kind of security, that kind, and the other... We have to divide the issues clearly: there is security for the individual: that is the first level. Children suffer the most. There is another level: that of corporate security, which companies themselves need to provide for themselves, to a certain extent. The next level is state security, which the state should, certainly, always safeguard. For example, the Stuxnet virus, for those who do not know, is a virus written under a joint commission from the Governments of the United States and Israel in order to attack Iran's major infrastructure facilities. The example of this highly complex virus, which analysts from around the world spent three months unpicking, shows that cyber-attacks by one country against another are possible. So, if a country does not defend itself against this somehow, it is at the very least stupid.

On the other hand, there is regulation. To simply announce that we will now regulate the entire Internet would be entirely nonsensical. We can, however, consider technical measures. We are under attack by technical means when people hack accounts, attack, and organize mass demonstrations on the Internet directed against the state. If we are talking about the state, then we can, in principle, fight back. With what methods? There is a filtration system, web filters, especially filters with linguistic technologies, which can easily handle it. There are firewalls, and new monitoring systems are now coming out which can monitor any kind of information. You enter, for example, 'terrorism', and they will check for all terms that are linked to terrorism or which might be used in place of the word 'terrorism'. Of course, they will give a certain number of false positives, but, in any case they will provide some kind of picture. I know for certain that the intelligence agencies of all countries are doing this. Of course, these filtration systems exist. They are used in surveillance and real work is being carried out.

Now and then, a few nasty sites are shut down; the battle is being fought periodically. How effective is it? Well, yes, they can crop up elsewhere. But if you do nothing, the result will be nothing.

In addition, I will answer Andrei's question about the danger posed by social networks. I have some figures on social networks. Here are the figures for Russia: in 2009, more than 130,000 vKontakte accounts were unlocked and made openly available. This is less than 1% of the network's users: about 0.1% of all vKontakte users. Next, if we take the world overall, the past year in particular was a breakthrough year, with more than 100 million user accounts made openly available on Facebook and Pirate Bay. Now, if Facebook has 640 million users, then 100 million is about 10%, no, strike that, nearly 20%. That is a lot. The same thing happened on MySpace and Facebook; the personal data of millions of users were transferred via commercial applications. In this case, another area of vulnerability was exploited, but the total number of attacks on social networks over the last year increased by 100,000. That was the number of attacks. And in a single attack, the information on one hundred million users could have been stolen. That is one attack. There really is a problem. But I am not going to talk about Sony, because the case has already been spoken about so much.

Because they bring a lot of people together in one place, social networking sites are very good bait and a good place to make some money. People want to be part of them, so there are a lot of people there. People enter a lot of information about themselves, they enter all their data, so, why not steal it? Especially if we combine that with data from their credit cards, which is fairly easy to do if a single email account is used. Done and dusted. We can steal both. We grab the password and embed a Trojan, which turns it into a bot hotel or something else, and off we go...

T. Kandelaki:

Natalya, I have to ask and, although you may not be the correct person to ask, I am sure that you have an interesting opinion on this. You spoke about how offline theft naturally migrates to the online world. If someone was stealing as usual, why not steal something on the Internet, especially since you can steal money there, as well? Here is the first question: you mentioned attacks—is there any information regarding the number of attacks discovered? It is important for people to know this in order to understand just how vulnerable we are. That is the first thing. The second is that, for example, every country has its own punishment mechanisms, depending on the law of the land. Different crimes are punished in different ways. What do you think, will all countries, in the future, have to come together in order to ensure that the penalties for Internet crimes are harmonized, or will that never happen? In some places, the penalties will be more severe, and in some, they will be lighter. And what do you think is the more correct approach?

N. Kasperskaya:

The situation regarding detection of Internet crimes is absolutely deplorable. Last year, a few dozen cases were solved. A few dozen gangs who were involved in distributing Trojans, writing viruses, hacking, and stealing credit cards were caught. This is a drop in the ocean. I cannot even say what percentage it is, but I think that it is one-thousandth of 1%. If we compare that with offline crime-solving, in the latter we are talking about percentages in double figures. After all, 60–80% of murderers are caught. Thieves and bank robbers are caught in 90% of cases. If you simply walk into a bank wearing a mask and carrying a gun, you are more likely to fail than you are to succeed. But online, it is the other way around, precisely due to the anonymity and precisely due to the way it is organized.

In addition, it is a system that works. But we need to understand that it is not organized crime. It is a swarm structure, like a swarm of bees. There are people who write viruses—the virus writers. They are out there somewhere at the bottom of the pyramid. They get money from those who commission the viruses. There are people who place orders online for virus writing. There are people who advertise these services. There are people who launder the cash, as it is dirty money and it needs to be extracted somehow. And the whole system works after a fashion, even though it lacks a single governing structure. But people say very often that Russian programmers are the ones writing the viruses. Russian and Chinese programmers often write the viruses, but the orders come from elsewhere. In other words, it is an international system. Last year, I think, they caught a group of Ukrainian programmers. Their base, where the work orders came from, was in New York, and the programmers just did their programming work .

You see, it is not even clear how to find them. Where is their centre? Who controls it all?

T. Kandelaki:

I just want to add that when we talk about classic robberies, we all think of the American blockbuster Ocean's Twelve. We understand that there is a customer and there are people who carry out the orders. And what you say shows, above all, that these people are very difficult to trace. But, since they are stealing databases, you may find yourself listed as a perpetrator of major crimes, despite the fact that you have not committed any. Do not be surprised if this happens. Have I understood correctly? You have published your information, someone stole your information, and a crime could be committed using your information, correct?

N. Kasperskaya:

Theoretically, yes, you could be a member of a botnet, and you would not even know about it. A Trojan just gets embedded and sits there quietly, and the traffic from your computer simply increases. And, and the same time, your computer is sending out spam or doing something else, under orders. Millions of computers are connected to botnets. And millions of unfortunate users do not suspect a thing. They are just victims of this situation. To imprison them would be unfair. What for?

T. Kandelaki:

Thank you very much.

T. Kandelaki:

My next question is for Mr. Peter Grauer. We return to the definition of privacy. Julian Assange said, "The best way to keep a secret is to not have a secret." In that case, I am interested. Do you believe in a world without secrets, in honest, transparent diplomacy, in honest, transparent business?

P. Grauer:

I want to make two observations. One is a little bit of an extension of what Orit said. I would like everybody in this room who is currently engaged in some activity on their cell phone, iPad, or tablet to raise their hand. Come on, tell the truth. You are not telling the truth.

Because I can see you, and the reason I can see you is because I have looked and your eyes are not on the stage at all when people are talking. So that is kind of an example of the magnitude of the problem. And if you look at all the photographers who are here, they are doing digital imaging, all of which will go on the Internet in some way, shape, or form within ten or fifteen minutes when we leave here. So that is the first point I want to make, just to emphasize the complexity of the issues and to some degree the way in which all of us kind of take for granted that these things are going to be protected or privacy is going to be okay, and I think it is incredibly naïve for us to think that.

The second point I would make just before I get to answering the question more specifically is that I had dinner about six or eight weeks ago with a former Chairman of the Joint Chiefs of Staff for the President of the United States. It was a dinner of about ten individuals and someone during the dinner said to General Pace (he is a four star general in the Marine Corps), "What are you worried about the most?"

And so, he started in Afghanistan, Iraq, and he went to North Korea, he went to Mexico, and drug terrorism, and he has been to every other middle eastern, every other hot spot of the world, and he said, "I do not worry about military terrorism anymore. I worry about cyber terrorism."

And this for all of us, whether you are in government or you are in the private sector, whether you are in business or you are in education, it is a topic that we have to, as a group of people around the world, wrestle with and deal with successfully going forward.

And I do not think that means they are hard and fast rules in the end, but I do think they are standards of conduct that have to exist across borders and there have be public-private partnerships that come together, to try and create some of those standards and accountability for people, in terms of what they do over the Internet every day.

We, as a company, and my firm, believes fervently in the concept of privacy—number one—which I do think can still survive, and number two, the issue of transparency. Because transparency creates, I think, a much higher confidence in those entities that are transparent with the information that they have.

And so, I do not think transparency is going to be a thing of the past. I think it is going to continue, but I think the responsibility is for all of us, particularly in our company; Elizabeth will talk about this in a minute as it relates to her company. We are one of the largest providers of information in the financial services community in the world today. If we go down because someone has hacked into our system, the capital markets of the world stop.

And so we spend an inordinate amount of time. Security in our company reports to me. I meet with our head of security two times a week to talk about things that are going on. We operate one of the largest private communications networks in the world. There is no way for any of us to, in any way, get in front of the tsunami that has been created, that we have all contributed to around the world, but we have to create some standards. There has to be a concept of privacy for all of us to feel confident that our information as it goes back and forth, whether it is between family members or colleagues or whatever it may be, can be protected.

So I am a believer in privacy. I am a believer, certainly, in the world of transparency. I will just digress for a moment. Those of you who have seen this: we wrote an op-ed that appeared in the Wall Street Journal today about the ECB and its unwillingness to disclose information as it relates to, specifically, the loans that it has made in Greece and the financial support for Greece. I think those things have to continue to happen, but I think we all have to be more vigilant, and there have to be standards.

T. Kandelaki:

We have one of the managers from Visa, Elizabeth Buse. That is why everybody will understand why my next question, of course, is about money. Everybody is interested in how they can save their money. There seems to be a lot more coverage of data security problems around the world.

Clearly, no company, I think, can guarantee the safety of their data. They get the feeling that millions of their clients are starting to feel more concerned about this. Is there anything that you can do, as the world's leading payment company, to renew this confidence? I think that everybody has a card here, and everybody is scared about this. Your money: safe or not?

P. Grauer:

Can I just say I think she does a great job? Elizabeth. You all know when you are somewhere and you get a call saying, "Did you really go to Las Vegas and spent all this money?" They are protecting you.

E. Buse:

Thank you very much. Today is the first time I have met him. Isn't this great? So thank you, Peter, for that, and yes, right, everyone does have a card, or everyone has an electronic means of payment, which says that we always need to balance the promotion and the growth of global commerce with security.

As a brief introduction, because I do not think it is widely understood what Visa is, so Visa is a global payment network. We operate in 200 countries and we process transactions in about 175 currencies. But, we do not set fees to merchants or consumers. We do not lend money and we do not maintain consumer-level data typically. That is with the bank who issued your card or with the merchant who accepts your card.

But within that context, what we are concerned about, as it relates to card transactions, is fraud. Someone gets my information and they can go make a purchase using my money. Well, it is important to dimension fraud. So if you look in the Visa system globally, fraud has been declining at the same time that payment volume has been growing in double digits.

Today, fraud is at its lowest level ever, at five cents per hundred dollars transacted. And on the Visa network, that is on the basis of five trillion US dollars that go across the Visa network every year. So while it is important, you need to know that it is something that is decreasing, and that is an industry we are all investing in very heavily.

So some examples of that are the payment card industry data security standards—PCI DSS for short—that is something that the entire industry has adopted—the financial institutions, the payment networks, the merchants—and they are globally consistent to make sure that we are looking out for consumer data.

Just recently, Visa came out with a best practice guide for the emerging technologies of encryption and tokenization that will make data even more secure. And as Peter mentioned, we are constantly investing at a very high level in our network to ensure that as we grow, particularly in the new channels like e-commerce and mobile, we can effectively manage fraud on your behalf.

In fact, today, every transaction that goes across our network is scored dynamically for risk and monitored for fraud, and that is every transaction in every second of every day. And I would just add that you have heard three words here repeatedly from all of the panellists: partnership, balance, and standards. So I will take those in different order.

Balance is really important, where I started. We have to be able to promote growth at the same time that we are mindful of security. That is the balance that we all have to strike. To achieve that, we have to partner. We need to partner with governments. We need to partner broadly across whatever our ecosystem is—the payments ecosystem in Visa's case—and we have to have standards.

We talked about the fact that the Internet is borderless. If we do not all have the same standards for security, for privacy, we are not going to be able to promote that growth.

T. Kandelaki:

I wrote a post before our panel began, about the blogger from Damascus, and I am receiving a lot of comments, perhaps even from people who are in this room —I do not know. I really liked one comment, which asked: "Which is worse: anonymity or total control?" And if someone from the panel could respond, it would be great. Then we will move on to questions from the audience. Actually, look how funny this is: here I am now watching what comments I am getting, and I do not know whether they are from people in this hall, or, possibly, from some other part of the world. And this is a perfect demonstration of what we are talking about today. In a nutshell, if it is not too much trouble, could one of the participants answer this question? Please answer. Natalya Kasperskaya.

N. Kasperskaya:

Yes. I think that the way the question was asked is all wrong. It is like two extremes: neither one is inconceivable. But total control of the Internet is impossible, simply in a technical sense. For that, you would have to completely change the entire system of the Internet, change the entire server hardware infrastructure. Right now the Internet is trying to move to the next standard, to version six, but that is no easy task. This is a complicated and difficult process that will take several years. To change the entire way the Internet works would be simply impossible. Complete control is simply impossible, given the current architecture of the Internet. Therefore, that kind of question is meaningless. In general, complete anonymity is also non-existent. If we look closely, people register themselves, people subscribe to some services, they make purchases and provide personal information. There is a great deal of this information and it accumulates, just as Orit said in the beginning. In principle, there is already a lot on every person. So it is impossible to say that it is completely anonymous. Sometimes, it even happens that criminals commit some kind of crime, and then it turns out later that he or they belonged to a social network, and that we can look to see what they are up to. I think that we simply need to observe some kind of balance with respect to control. We must clearly understand the threats we face, and protect ourselves from these threats.

When a company thinks about how to protect itself, it first builds a threat model. It is the same story here. We need to build a threat model and protect ourselves against this model. One model at the state level, one model and the individual level and a third and the corporate level. That is all.

T. Kandelaki:

Спасибо. Orit, please.

O. Gadiesh:

It is interesting: I already said there has got to be a balance; I was actually probably the first one that said when I started. But it becomes words, especially when Internet providers or providers of technology and technologies don't actually tell you.

The recent thing with Facebook, for example, with the face recognition, which people were not informed about until after. And then they had to be told there is a button to undo that. Now, it was done because, obviously, Facebook wants to connect more things and make more money; that is their company. That is where the battle actually is, because if I want to protect myself—I do not do any social network; I am not interested. I have gone on one or two anonymously, not with my name, just to see what happens on it, because it is interesting from a commercial point of view to understand that. But the battle, actually, that is going on is not only between countries or between people who want to do crime, but between the people who are developing the technologies and the people who, like Peter and I, who care a lot about privacy, and who do not even know, perhaps, what is being done.

And quite a number of those companies had to retreat back under pressure from their customers who were quite irate or quite mad. The people who trusted Sony did not, obviously, know that, unlike Peter, who sits twice a week with his security, it must not have been happening at Sony, because we now understand what is happening. So it is a very complicated issue. I mean, to say “there needs to be a balance” is relatively easy; that is clear. That is what democracies have done over the years, and there are also special punishments for people.

And Interpol, for example, exists for—but you cannot create the balance when there are too many different entities that want too many different things and are actually fighting.

And that is what the eG8 was really all about. They spent four days and they came to the conclusion that they completely disagree. You keep saying there needs to be a balance. The only thing that I need to protect myself is to put as little information as possible: that is, everybody is up to their own—but even there I may not know, as the people on Facebook find out.

So how do you see the beginning of creating the balance? Where does it start? Right now, there is nobody who can give an answer to that. The issue is becoming much more extreme, as Peter said. I think cyber terrorism actually has been one of the biggest issues now for quite a number of years; it is not new. But there is not any entity that can actually edict anything. There is no agreement between so many different entities.

N. Kasperskaya:

I may actually answer this question, because just recently I came from a cyber security forum which was created by the West-East Institute. It is trying to organize some place to start at, to do something about cyber security.

That one was the second one; it was held in London. The first one was held in Dallas. The whole idea around it is exactly to address common threats, because there are too many common threats for everybody. And there is a need to do something about it. So you were talking about the governmental level: then, I agree, the interests are different.

So China would probably not agree with the United States and with some other countries. Russia will also maybe disagree on something. If you put all eight countries together on the governmental level, it would probably fail.

On the other side, there are public organizations; there are private companies; there are private people. Still, governments must protect all those entities. We all have the same kind of threats which we need protection from. Again like, child pornography, or like cyber terrorism, or like—I don’t know—botnet creation or credit card data stolen, etc. There are still plenty of things to be done. The countries are trying to agree; the experts are sitting together and trying to figure it out. Actually, at the last Forum, a big part of the Forum was devoted to definitions. The main problem they discovered is they have different definitions.

They do not know what they should define as a threat. Is this a threat? What kind of level of threat? They had different workshops and definitions. So maybe after the definitions will come the next stage, where, at last, countries will come to some agreement.

At least, this is my hope, because by technical methods, it is already absolutely clear. It is not possible to cover that massive number of attacks all around the globe. It just absolutely impossible. So we need to do something together with the public, private people, and the government, and most especially everyone involved, including education for the private sector.

O. Gadiesh:

But the one thing that you did not mention in this thing is, again, companies who want to make a profit out of being able to use data. It does not seem to be illegal—we are talking about privacy here—it does not seem to be illegal until people just protest because nobody told them before.

So it is not just between countries. I think child pornography… most of the world sort of agrees it is not a good thing to have, but there is an issue between people and entities that are making money that was not possible to make before, because they can make connections that nobody could make before. And they are not punished for that because it is not punishable.

N. Kasperskaya:

I suggest the following. There are many threats. The total number, for example, of just existing viruses is more than 50, different types. So, if you try to protect against everything, it will be an impossible task. What the world should start with is to define the areas where we can do something together and try to protect those areas. You are absolutely right about privacy, about companies who want your money. Maybe we should postpone this problem for a while, because there are many more issues that have to be solved. And start to solve some problems, because there is a huge number of problems to be solved still. Step by step, we slowly—I believe—will improve the situation.

T. Kandelaki:
Thank you, Natalya.

E. Buse:
If I could just add one quick thing, because I think what Orit I was saying is really important, and that is that consumers have, clearly, an expectation of data privacy and, I think we all agree, a right to data privacy. And even if that data is not misused, I think they are entitled to be aware that someone has their data and be given a choice about how that data is going to be used. This is back to your Facebook example. They should be asked and be allowed to say "no".

T. Kandelaki:
Thank you, Elizabeth. Now, audience, if you have a question, we have time only for two questions. I am so sorry.

From the audience:
This is a question for Orit, Elizabeth, and perhaps Natalya Kasperskaya. So, basically I'm in a tech business and there are a lot of hackers, and the hackers

are not really there to break into systems because they want to do it or they are terrorists, but they are doing it out of curiosity.

My question is, from an entrepreneurial standpoint, have you ever thought of creating a fund that would empower these people to create companies that would create a new level of security for your companies?

O. Gadiesh:

Actually, that is being done. I mean, a lot of those people are hackers who have been recruited to become entrepreneurs to help us figure it out. So, that is something that I think has been done for a long time, but there are experts here who know more about it than I do.

E. Buse:

I will just add, quite briefly, that I think what you have seen about companies opening the edge of their network… obviously, this was led with—like the developer centre on Apple. In Visa, we have opened up the edge of our network and encouraged development both of applications that would spur consumer use but also data security applications.

P. Grauer:

I would also add that I think any company that thinks about these issues seriously engages outside firms to constantly do penetration testing in different ways to penetrate their firewalls and networks to see what the implications are and ultimately whether they get through or not. I think there are groups of people who are doing that.

T. Kandelaki:

Fritz Morgen, the famous Russian blogger.

F. Morgen:

My question is to Natalya Kasperskaya. Tell me, if you had the technical capacity to snap your fingers and eliminate anonymity, well, for the sake of global security, for example, would you do it?

N. Kasperskaya:

No, of course not. Eliminating anonymity would lead to problems of another kind. Here, in fact, we are talking about the fact that the loss of privacy is a terrible thing. Now, let us imagine that there is no anonymity: a person has already posted a lot about himself and practically everything about him is out there: where he has been and what he did there. I even know of cases where social networking has led to dire consequences. That is why I think that the Internet is just what it was created to be. There are pros and cons, but let us live with what we have.

T. Kandelaki:

Well, here we are talking, and for the first time, the following thoughts have come to mind: to what extent did the emergence of the Internet lead to an increase in crime, statistically speaking? Previously, after all, people were somehow restrained, not only by moral norms, but also partly by the law; by the understanding of the penalty they would pay for committing a crime. The Internet now allows people to express their aggression. You can say what you want and inflict whatever harm you want upon whom you like and nobody can do anything to you. I think that it is impossible to fit this topic into one panel discussion. We could talk about this for ever and a day, because with every passing minute, with every passing second, there are new possibilities emerging for ever greater communication between people all over the world. It seems that the closer we get, the more vulnerable we become. Here it is—the global world, about which we have said so much, towards which we have been striving. We wanted to live in a global world, and here it is. At any moment, we are now able to contact anyone we want, using Skype. But what it will bring us is a different question.

Many thanks to all the panel participants. Thank you, ladies and gentlemen. I would like to say a few words. Well, first of all, it is clear that Russian hackers were with us today in spirit. And I am absolutely convinced of the fact that you will be leaving today feeling a little less secure and a little more vulnerable. But that is life. You chose this panel, so there is nothing you can do about it: you will have to pay the price.

Since I have worked in television for many years, I cannot help but recall one thing. When television had just appeared, many criticized it for putting pressure on people, forcing them to make choices that they did not intend to make. We would like to choose one thing, but the television convinces us to do something else. But what is television? Today, the Internet gives us the ability to influence people and we do not even know that we are doing it deliberately. This is the fundamental difference. In television, we know what we are sending your way and what we want from you. But on the Internet, when we send somebody something (and I am not talking about large companies which need to make money, but personal communication), nobody can know where that communication will lead. Do you know the excellent phrase, "This spy camera never sleeps"? So, when you hear, for example, that the Internet is a tool of Satan, you realize that there are fewer and fewer of these people, because it is impossible to resist. You just need to learn to live with it. That is the most important thing. So I am sure that humanity will find a regulatory mechanism.

History recalls instances when entire peoples died out from disease, but, nevertheless, something was then restored, the mechanism was rebuilt and humanity preserved itself. The self-preservation mechanism in humans is too well-developed to not take advantage of this amazing opportunity which has, in the space of 45 years, given us something that that the era of the prophets and the arrival of literacy were unable to provide. That all goes back thousands of years. The Internet only goes back tens of years. Thanks are due to Peter Grauer: I have to say that I could not help but notice that everyone raised their hands when he asked who is a member of a social network. You all answered honestly to say that yes, you were registered. So, Peter, if you do not mind, allow me to ask all those who raised their hands to be sure to follow me on Twitter, and I hope that you will also do so, as I am subscribed to Bloomberg News.

Thank you very much.