



## DEBATE

### **Karl Kaiser, Harvard University**

Carl, you made a very important point about two major advantages of the US over Europe, energy, and big data. Are you saying that in the long run Europeans have to give up their concept of privacy, which is very different from the American concept of privacy in order to regain an advantage? Europeans themselves have very different cultures when it comes to privacy. Could you explain the long-term approach?

### **Sergey Karaganov, Honorary Chairman of the Presidium of the non-governmental Council on Foreign and Defense Policy of Russia**

Could you go one step further? What does that mean for the social and political structures of the world? It is not only the IT revolution which is speeding up. It is also about robotisation, which means that in 5-10 years most manufacturing jobs will be not only be outside Europe but also outside China, which will create a totally different world, a world of totally different social tensions, and these will underlie the politics of tomorrow, which will be quite different from now. Could you address the social and political consequences of what you are talking about?

### **John Egan, CEO, Sandbox, London**

Does this migration to online communities signify a fundamental decline in the unifying power of the nation state? Is what a lot of people see as the apathy of young people about politics an affinity that crosses borders through technology?

### **Fred L. Smith, Founder and Chairman of the Competitive Enterprise Institute, Washington DC**

Following on from the first question, the European concept of privacy seems to be that information about yourself should be walled off from the rest of the world; the American concept is that privacy is a voluntary sharing of information of those you contract with. It appears that the European concept of privacy grew out of the misuse of government acquired information in the 1930s and World War Two, and it has not been rethought to recognise that a voluntary exchange of information with whomever is perfectly compatible with privacy. Europe seemingly has to make a decision about that, or it will forego the advantages of big data, which will be very harmful to your economy.

### **Thomas Eymond-Laritz, APCO**

Assange and Snowden brought a real revolution in the West, especially in the US. Do you expect other people to act like that, not only in the US but also in other parts of the world, such as Russia and China, and what would be the consequences of that?

### **Abdulmajeed Al-Shatti, Former Chairman, Commercial Bank of Kuwait**

Can we apply the laws that we have today to the new technologies, or do we have to invent new laws for them? Secondly, how can we, as individuals who use social media and new media, monetise the content we put there, what rights do we have, and who can protect us as users?

### **Mohamed Laichoubi, Former Minister, Algeria**

Sur la question sécuritaire classique, nous avons attendu une évolution assez importante avant de voir le débat de la sécurité concerner toutes les grandes institutions multilatérales et la coopération internationale. Ce que l'on relève maintenant dans les questionnements c'est que c'est plutôt des défenses nationales sur la question du cyberspace et



la cybercriminalité qui sont plus développées. Est-ce que vous voyez en la matière une nouvelle philosophie internationale mettant en intervention les institutions du type ONU qui commenceraient à se réformer pour se préoccuper des grandes questions liées à la liberté et à l'organisation d'une sécurité multilatérale ?

**Carl Bildt, Minister of Foreign Affairs, Sweden**

The privacy and data protection issues are exceedingly complex and important, because they have vast implications for competitiveness and other things. There is a generational divide; how you would define the US approach is how a substantial part of the younger generation in Europe would define it, because if you sign up to Google or Apple or whatever, you tick the box and say 'I agree.' It is a fairly long text, and it is fairly small print, but you do tick the box and agree that your data is used in some sort of way, and that is fairly okay from a legal point of view. Should people not have the right to do that if they want to do it? I think they should, but we should make certain that they know what they are doing, and in that case we should have a gradual merging of the different European approaches with the US approach, because otherwise we will be in trouble.

We have different histories in Europe. France has a tradition which is different from the German one, the Swedish one, etc., and this will have to be sorted out. This is one of the reasons why the European Council was dealing with the telecommunication regulation issues, data services, etc., one or two months ago, and decided it was too difficult and to defer it to 2015. I think that was wise, because we need more of a debate on it, and it is a question of long-term competitiveness. There are areas where we have a huge competitive advantage in Europe. We have national health systems, which means we have national databases for the health of our citizens; if we use big data technologies there, we can learn enormous amounts in order to create enormous advantages in terms of health, which the US cannot do.

Regarding apathy with politics among young people, I do not agree. There might be apathy with politics as performed, but I see a rising interest in issues, including global issues, because young people now connect with issues to a much larger extent today, not with the policy packages of parties to the same extent as used to be the case, but with the issues, and they can connect to the issues and learn about them in new ways. Therefore, there is a rising interest in the issues of politics, not necessarily with the classical instruments of politics.

Regarding global governance, it will be affected by this, needless to say, but we need to understand that we need an agreement on basic principles, not necessarily to change them. Protection of freedom should apply online as well as offline, not that every country respects it. We should respect the independence of business. We should respect the right of individuals to their privacy, but they can dispose of it in their own different ways. Then we must look at where it is heading. Where are we heading? I do not know. We are heading towards a much more dynamic environment, and accordingly, much more unpredictable, but the societies that will prosper are the societies that have an incentive for innovation. The most snappy societies and economies are the ones that will be ahead 30, 40, 50 years down the road; the static ones, the regulated ones, are the ones that will lose out.

**Paul Hermelin, Chairman & CEO, Capgemini**

There was a question as to whether an Assange or a Snowden could come from China, Korea, or France. We probably had one in France already. That would be my first question. Secondly, today we talk about a digital war. Is that totally national, or can we see global organisations dealing with that?

**Meir Sheerit, Member of the Knesset, former Minister of Intelligence Services, Israel**

Firstly, the Internet is here to stay. We do not have the option, as people once imagined, of turning the switch off. There is no kill-switch for the Internet, because we cannot manage anything today without the Internet. The problem is how countries can defend themselves from attacks and still function; it is not enough to defend yourself against attack, but you also have to keep your Internet systems, as otherwise you cannot operate yourself. It is here to stay. Our friend from Kuwait asked who is protecting us. No one is doing so. You can buy forms of protection, such as antivirus and so on, but you will never believe how easy it is to get into your phone, listen to every word you say, or intercept any SMS you send.



Maybe if we have another discussion in the future about cyberspace, I can bring someone who will demonstrate how easy it is to intercept your phone, no matter where you are, even if you switch it off, and listen to every word you say. It is unbelievable. Therefore, if you want to protect yourself, keep everything secret that you want to be secret; do not use any smartphone or any computer, because everything is exposed and nobody is really protecting you.

Regarding whether there are going to be more Snowdens in places like China or Russia, I think so. It is a matter of time. Snowden is an example to a lot of young people working in these systems to come out; it happened with Snowden and it can happen again. Last but not least, governments also have the ability, especially big and sophisticated governments, to intercept any of your phone calls by satellite. The US Government is a very good example; if any government wants to see what you are doing, with whom you are speaking, what emails you are sending, they can intercept everything you do, 24-7. The possibilities are almost unlimited.

There is no legislation in the world today about cyberspace. I think we need it. Carl said before that, from the point of view of justice, when there is a cyber-attack, under the regular law of war, when someone attacks you, you have the right to defend yourself with any means you have. Cyber-attacks are still not defined under law, and they should be defined. Today there is a lot of cooperation between countries, and from our point of view at least we have cooperation with many countries in the world, especially Western countries, in this area, but we should create some kind of global governance structure in order to find out different things each country should do or not do.

**Paul Hermelin, Chairman & CEO, Capgemini**

Mr Chang, the question was what would be the social implications of the digital world. Seeing that from the media angle, what can you tell us as a conclusion?

**Chang Dae-Whan, Chairman, Maekyung Media Group, Republic of Korea**

I would like to address three questions, the first one being on the privacy issue. There is no privacy whatsoever, so be prepared to live without privacy. You are checked everywhere as long as you carry these smart phones; you might get checked every 5-10 minutes wherever you go. You will buy a smart television, and I am sure you will enjoy watching it, but in the meantime the set-top box will watch you and whatever you do in your room. Therefore, privacy is gone for sure, no matter what you do.

Regarding the monetisation issue, intellectual people such as those sitting here are more than willing to pay for content. I launched an e-paper several months ago, and I already have 20,000 subscribers who are paying about USD10 a month; I hope to increase this number to 200,000 in several years. Therefore, people are more than willing to pay for what they have, if it is a good service, so monetisation will continue.

Finally, somebody asked about the social consequences and the challenges in the Internet space. I think we need to worry about the social disintegration that might happen. Yesterday morning at the opening session, economists talked about the unequal economy, the gaps between the rich and the poor; I think these will increase and expand. Someone, I think it was Professor Tyler, checked on this issue. It used to be a 20-80 society; 20% of people overtaking the other 80%. However, the numbers will be different in future; 15% will thrive and the rest of the people might suffer a little more. That is my answer to these questions.

**Paul Hermelin, Chairman & CEO, Capgemini**

I will say a few words in conclusion. Capgemini has put digital transformation at the forefront of its mission, and the digital transformation of the world is accelerating. We will have to understand the roots of what we might call digital welfare and digital diplomacy. Military people understand more and more about digital defence, and a bigger and bigger share of military budgets are now allocated to cyber-defence and global digital governance, so my bet is that this question will come up more and more in the agenda of the seventh, eighth and ninth World Policy Conferences.