DEBAT

Nicolas Barré, directeur de la rédaction, Les Echos

Thank you. I would love to take one or two questions from the audience if we have time.

Anil Razdan, ancien ministre de l'Energie de l'Inde

It was very interesting to hear, I think, two conflicting viewpoints on big data, but I think my question is does big data really protect privacy or liberty of an individual, what are the guarantees against it, what about the menace of hacking unwanted solicitation and, I think, snooping? It gives the impression unfortunately today that you have a spy camera in your bedroom if not your washroom or are we living on a nudist beach? That is what I would like to ask the first two speakers, how do you protect an individual? I think in this part of the world we are already going through a controversy of a controversial film being hacked and what can be the consequences of it? How do we bring about that balance? I would entirely agree with the last two speakers, Ben and Mr Nye, that people are beginning to be highly suspect of these devices. Because as talking of 1984 George Orwell, we do not want Big Brother watching us all the time or somebody bothering us when we do not want to be bothered.

Nicolas Barré, directeur de la rédaction, Les Echos

Okay, can we take two other questions in the front here please because we will not have much time for discussion afterwards?

Jean-Claude Trichet, ancien président de la BCE

I was fascinated by Joe Nye mentioning that we had a Panopticon in our pocket. It seems to be that a Canadian academic gave this capacity for all of us to surveil from behind. The expression of, sousveillance, you have surveillance and you have underveillance, if I may, sousveillance. It appears at first look as introducing symmetry. We have Big Brother on the one hand but we have all the small brothers that have their Panopticon in their hands and could surveil and we see the effectiveness of such sousveillance when we have the police doing something which is very abnormal, then clearly it is the Panopticon which functions, and is spread the world over through all TV networks. Is it balance in the view of Joe or is it still very unbalanced? Thank you.

Meir Sheetrit, membre de la Knesset ; ancien ministre responsible des services de renseignements d'Israël

I think that big data is not a matter in which is people are threatened by governments; it is much more by companies. The companies are so trusted, to more and more data for every person and everyone who uses their services. Whenever you buy anything in a supermarket and you pass your credit card, so the supermarket have all your details in this credit card and they are collecting more and more, as much as they can know about you. Therefore, in the situation of today, the big data, the main big data are in the hands of companies. The question is are those companies using this data for what? They do. I am not wondering if anybody of you getting for example from the companies of supermarkets from time to time you get the discount on the things that you usually buy in their supermarket, because

they know exactly what you buy, they can connect to you, they can suggest to you a discount for what you buy so that you buy more.

However, more than this, they try to get to know more and more about you. There are companies in the world which collect this big data and they are trying to reach those big data and make out of it integral about all your data from different places, banks, supermarkets, whatever you use, they get everything about you. This big data is totally not controlled by governments. As a matter of fact, in my opinion, if we want to protect anything about privacy of people, one of the things that government have really to put a hand over those big data resources. According to the law there are some laws which say that every data space should be controlled by government. In matter of fact, the reality of this supervision is quite zero. Today you have to take in consideration when you want to buy anything, people ask you, when you fill in a form, and when you put a tick under, 'Do you want us to send you updates?', say 'Yes', 'Where do you live', 'Yes', my address? 'Yes.' Everybody does not think about it and says yes, yes, yes. All those answers collected. You have to take this into consideration because you have some control about your data. Whenever you fill in a form, think what you want people to know about you, what you do not want them to know about you. Everybody has to make this own consideration, otherwise you are giving all your privacy to other people to be held by other people and governments and so you say, governments are totally not protected, they even cannot in many countries in the world, they cannot even protect themselves.

Just lately, I do not know if you know, but there was a very big meeting between Obama and President of China in order to try and reach an agreement about cyber between the two countries, because America sees the Chinese as one of the biggest attackers in cyber of the United States, and therefore there are examples, just lately in 2013 the United States got a warrant, the defense ministry of the United States, the secretary of the United States got a warrant not to buy anything which has any IT from China. I wonder if you have any other ideas what to do in order to control this big data by private companies. Thank you.

Nicolas Barré, directeur de la rédaction, Les Echos

Okay, so who would like to start? Luc- François?

Luc-François Salvador, président exécutif de l'unité Asie-Pacifique du groupe Capgemini

I am going to be honestly blunt, but when you ask a question about is privacy protected, what about hacking and all that, the answer is in the question. However, the answer as well is related to the paradox Ben put on the table. How many of you in this room would accept to be disconnected from their email for how long? One day? Two days? One week? When would you start becoming dysfunctional because you are not connected? At the end of the day, and I say that without any cynicism, we are paying what we are asking for. No privacy is not possible. The avenues on which some of the legal thinking or parliamentary thinking is about is, could we formalise legal situation where we do not look at any individual data but we look at average, in other words, if I measure the behaviour interconnected of an individual, I could get away by measuring the average behaviour as opposed to a given individual. Those are some of the avenues which are being explored, but we have to accept that we are the ones who are creating the problem by the fact that we are reachable, connectable and as the gentleman was saying, we even answer yes when the question is do you accept to be located. We say yes. A lot of us at least.

I have a very poor answer on the companies' data, it is that for the moment we do not know how to treat the data because we have too much of it. I gave you the number of 12%, we cannot work on 88% but there will come a day when we will be able.

Ben Scott, conseiller principal, Open Technology Institute à la New America Foundation ; directeur des programmes, European Digital Agenda, Stiftung Neue Verantwortung

I think just as we are in a process of catching up, as Joe put it, with the power of technology in the realm of intelligence policy and security policy, we are also catching up when it comes to big data in economic policy, in privacy policy. Obviously big debate in Brussels right now on the European Data Protection Directive, but the problem with all privacy rules in the big data environment is that the second you click that box that says, 'I agree', all those protections are gone. We have not yet figured out a way to judge at what point is it reasonable to apply protections that guard against things people have agreed to. There are very different philosophies in different parts of the world about whether you should do that pre-emptively or whether you should do that ex post facto. I think that is the state of the debate at the moment.

Joseph Nye, Professeur émérite, Center for Public Leadership, Harvard Kennedy School

I am going to go quickly on each of the questions. The first question, big data is here to stay, that was the point I was trying to make, that it is not the revelations of Snowden, it is not what NSA did, it is intrinsic to what the capacity of computing power has done to our ability to make social choices. Therefore, the key question is how do we develop procedures which exert some controls, which do not allow us just to be the prisoner of Big Brother. In China it is not going to happen. In the US, in Europe, it should happen. We are only partway there, but it is something we have to do. On the Sony hack, that really is not a product of big data, that is a different problem that we do not have time to go into here.

On Jean-Claude's point about sousveillance, which is a wonderful term, you can use some of this technology for protecting civil liberties. After these terrible events in which police have used excessive force against young black men in the US, there is now a movement, President Obama suggested it and having the government pay for it, to have the police wear little lapel cameras. If you are a policeman and you are tempted to do something violent and you know that this little button in your collar is going to record it, you might be a bit more restrained. That is a great example of sousveillance that you mentioned.

Then third, on the question of companies, one of the problems that we do not pay enough attention to is that it is not what one company does, it is when you combine data from many companies that you can do a lot more damage. Companies will say this is anonymous; we are just collecting; we are not identifying you. It is not that hard to de-anonymise when you have several data sets. Indeed, I was talking to a person last week, who is in charge of data at a large European, not American, European advertising company. He said, 'We find that we are constantly de anonymising so that we can go at specific customers on what to sell.' He said, 'One of the biggest assets we have is Facebook.' He says Facebook is not a communications company; it is an identity seller. Because once I can get enough information that I can combine it with Facebook, and I open that up, and on Facebook you have told me everything I want to know. Who your girlfriend is, where you spend your vacation, your dog's name, and so on and so forth. Notice that has nothing to do with Snowden, nothing to do with the United States, this is a European company. Therefore, the problem of big data and how we control it is much bigger than the NSA.

Chang Dae-Whan, président de Maekyung Media Group, République de Corée

As a newspaper publisher I print about one million copies daily and including two TV channels and Internet service, I have an audience of about 15 million. I get texts from hackers every day, I get about 20,000 hacking trys every day, so I have anti hacking business units in my companies, so that is how I protect my services, like television producing units, 100% separated from outside. My printing press is also structured that way. Every single person in this room, try to collect data. Try to collect more, that may be the possible answer in surviving this area of competition.

South Korea is still a divided country, North and South, the communist North and free country in the South. Therefore, the Snowden case did not catch my interest. I mean, spying, jobs and espionage things, I mean, it is everyday life. We live with it. We live with this world of Panopticon. Third answer, we do not care and there is nothing to do, so that is how most Koreans face this problem. However, do not be too pessimistic with the big data future. Big data will be a

very useful in transporting and forecasting and we are going to have more accurate statistical findings. How about trying oriental divination, based on big data? I think the future will be much more interesting as we develop through big data collection.

Fen Osler Hampson, directeur du programme de sécurité internationale et politique du CIGI ; co-directeur de la Commission mondiale sur la gouvernance d'internet ; professeur chancelier à l'université Carleton, Ottawa, Canada

Gentlemen, a terrific panel and Joe, thank you for the commercial, that survey of 24 countries is available on the CG Global Commision website, ourinternet, O-U-R, internet.org. You can find it there in all of its detail; it is a fascinating story. My question though is a simple one. Ben, you mentioned the push to encryption, particularly computer to computer encryption or platform to platform encryption; is that going to crimp the move to big data as we see the marketing of various kinds of privacy services, it will make data collection much harder, with technological innovation. Those of you who are in the big data collection business, are you worried about it?

Ben Scott, conseiller principal, Open Technology Institute à la New America Foundation ; directeur des programmes, European Digital Agenda, Stiftung Neue Verantwortung

My answer is it depends. For individual companies who are encrypting their own traffic using standard technologies like when you look at your browser and it says https, that is an encrypted connection, but the company that is offering the service has the key to decrypt the data once it arrives in their server, so for individual companies encryption that they provide for their service will not be an impediment to predictive analytics or big data business models. For intelligence agencies that pick up data off the wire, if the encryption is strong enough and there is enough of it on the network, it could change operational practices. I think it is likely that over time we will see interception technologies that move down from the software layer into the hardware layer, so that data is intercepted before it is encrypted. That is perhaps a cynical perspective, but over time I think that is where it is likely to go, but that is not to say that an encryption is not an important development, I think it is. I think it is one that should be interesting for market development, are there advantages to putting a product out there that has strong encryption or is it a reduction on the efficiency of data processing because it is costly to apply encryption overlays?

Joseph Nye, Professeur émérite, Center for Public Leadership, Harvard Kennedy School

I agree with what Ben said, but it is worthwhile, as you think of security, to realise there are three vectors of attack. We always focus so heavily on the network that we think that if we encrypt what is on the network we solve the problem. There are two other vectors of attack. One is equipment, the chips that are in your machinery that make you have to pay attention to the supply chain. There may be thousands of components, some of them are from China, some of them are from Malaysia and so forth, and if you put a back door in some of those, that may be even more effective than trying to break encryption. The thirds is humans. If you can corrupt a human, a Snowden, or a simple systems operator, you can bypass the encryption as well. Therefore, the better encryption gets the more intelligence agencies will be driven to the other vectors of attack in the supply chain and the human agents.

Nicolas Barré, directeur de la rédaction, Les Echos

Thank you very much, thank you gentlemen. That is a great conclusion; next session at noon on Asia and the US.