Lunch Debate

Privacy after the NSA revelations

The revelations by Snowden about the NSA practices have been mentioned a number of times during the conference and in the keynotes these days.

The lunch debate was moderated by Kim Cameron (Distinguished Engineer Microsoft). In his introduction he referred to his Afterword published in the DEF Yearbook 2013. He particularly mentioned the argument suggested in the political debate that metadata is no personal (identifying) data. That there is no content in the database that holds the data collected by the NSA, or said differently: it is all about “contentless content”, just identifiers like phone numbers, but no information on the conversation. Not surprisingly he strongly disagrees and claims: “The identifying numbers that are used to connect people and things to the content located in a staggering maze of databases are the key to the structure of the digital world.” He encouraged the various lunch tables to discuss these matters.

Some specific tables addressed specific angles to the topic and reported back.

**European Policy** (moderated by George Metakides, President DEF)
Reciprocity in market access (e.g. America Movil using monopoly rents to shop in EU); security and autonomy in the wake of political responses to Prism (e.g. Euro Cloud, data protection). How to align the need for security of the citizens with their need for privacy and control on the management of their personal data.

In this context the issue of free trade and the EU-US negotiation on this was tabled. How can we talk as equal partners about free trade if there is a clear power a-symmetry, created by backdoors available to one and not to the other. If one international party can create such advantages how can we build trust internationally?

**Technology Innovation for Trust** (moderated by Willem Jonker - CEO ICTLabs, EIT)
Can technology innovation help to build trust of citizens in technology use, in particular for security systems (incl. surveillance and legal oversight, personal data management, control and transparency)?

It was concluded that non-trust is in fact a blocking facto for innovation. And trust is undermined by a drive to centralisation, monitoring, profiling, “always on”. Perception of moral integrity and safety is essential for trust and this can be strengthened for example through: reasonable transparency, use of encryption, proper authentication, access usage control and reputation systems.

**Opportunities for Europe’s Internet industry** (moderated by Mario Campolargo - CNECT, Internet freedom, neutrality. Can security of citizens be aligned with it? Would adequate surveillance of the Internet be possible only in the endpoints or would technology in the
nodes be needed? Are there new opportunities for European Cloud Providers and Web entrepreneurs to benefit of the more privacy friendly European environment?

It is believed that the Snowden revelations indeed provide new opportunities for European Cloud Providers and Web entrepreneurs to benefit of the more privacy friendly European environment? This could change the competition picture. Already exist in Europe innovative small companies that focus on new ways to protect privacy by increasing user control on data and building trust frameworks for service sectors or groups of citizens.

**What can ICANN do?** (moderated by Nigel Hickson - ICANN)
What can be the role of ICANN in the debate of surveillance on the Internet. Can domain name management play a role in improving the situation.

The discussion had made it clear that the revelations of data surveillance has created tendency for individuals and businesses to change their attitudes vis-à-vis the US also at the level of Domain Name management.

**US policy and international cooperation** (moderated by Peter Brown (US Identity Ecosystems Steering Group))
A US perspective on Identity, privacy and citizen security. What is the direction the US chooses after the Snowden revelations. How can the US Identity Ecosystem help in better user transparency and data management? How can standardisation help?

The table discussed the so-called “magic triangle” for trust and progress: technical feasibility, social desirability, and consumer/citizen acceptance. Trust cannot be engineered by technology only and one must take a balanced approach to all three corners of the triangle. Moreover, one should no longer think linearly. In particular one should start thinking about “Value Networks” instead of “Value Chains”.

**Privacy friendly Security technology** (moderated by David Francis - Huawei)
Internet security technology designed and build with privacy in mind. How can Privacy by Design, Privacy Impact assessment, PETs be further developed to strengthen personal and legal oversight on use on personal data?

Development of privacy-friendly ICT and data security means countering the Surveillance Agencies. We have to come to arrangements in which optimal security can be implemented at all levels, whilst reasonable action can be taken to safeguard society against crime and terrorism, under proper political/judiciary control. It should be transparent which actions on which data and under which control can be taken to protect our societies against abuse.

Hearing the reports from the tables, the Chair concluded that the discussions made it very clear which complexities we face. There are no easy solutions for many of the issues brought forward in the discussions. Broad societal debate is required to develop step by step a “Digital Social Covenant” between Government, the Private sectors and the Citizens that will (re-)build trust and guarantees autonomy and freedom of the individual.