PERSONAL DATA MANAGEMENT IN THE DIGITAL AGE

Objective of the proposed session

Digital technologies have a deep effect on how people behave, think, interact and socialise. The management of Personal and Behavioural Data (incl. on health, education, interests, etc.) is central to these changes. Issues that are high on the agenda are:

- who has the right to collect and on which conditions
- how can the individual have control to ensure a certain autonomy in developing his identity within society.

The collection and exploitation of "Big Data" for targeted advertising and services, surveillance and profiling for forensics and law enforcement, or for health research and social sciences, lead individuals to lose trust in business and public organisations, due to a lack of understanding, transparency and control. Data that has been collected for a consented purpose are kept, combined with other data and use in totally different contexts. The Network session aims at discussing collaboration in this field to engage in activities to understand human behaviour in the digital age through multidisciplinary coordination and debate, and to do research and development for innovative and trustworthy solutions. Solutions that will bring back data-sharing in society under control of the citizen have special attention.

Agenda

1. Jacques Bus (Digital Enlightenment Forum)
   Jacques presented the objectives of DEF and gave an overview of ICT-related topics in Horizon 2020 which provides opportunities to community building in line with DEF objectives.
   This includes: Collective Awareness Platform activities, Web entrepreneurship stimulation, Big data and Open data innovation, IoT and connected smart objects and the Human-centric Digital Age.
   DEF is certainly interested to play a role in such activities with the multidisciplinary network of experts it has through its members and supporters.
2. Paul Malone (WIT/TSSG, IRL):
   Paul argued for development of an economic market place for user data access and service offerings. It should ensure transparent and accountable data access and usage and give clarity to citizens on the value of their data.
   He invited socio-economic research organisations, service providers, data brokers, relevant user groups and organisations working on virtual/community currency to work with him on this.
3. Phil Archer (W3C / ERCIM, FR): *W3C's strategy for Data Standards on the Web – From Open Data to Personal Data*
   Phil focused on general rules in the Internet for building Trust. Standards and protocols are needed to ensure a basic trust layer (Trust Framework) that can allow building more context-aware layers on top of it.
   He invited organisations to help him achieve that through proposals for Research and Innovation for Horizon 2020.
4. Luk Vervenne (Synergetics, BE):
   Luk was replaced by Katrin Franke (UC Gjovik, NO). She explained current activities to build Trust Platforms/Networks, particularly in Health. Essential elements (based on the TAS3 project funded by the EC) are: high-level data security in storing as well as processing; processes and rules that are well described and agreed between the platform partners and implemented through technology, incl. sticky policy, transparency and accountability to all partners in the platform (providers as well as users), and well designed governance based on balancng interests. More research and innovation is needed to ensure interoperability of such sector specific platforms in an overall ecosystem, and to demonstrate economic feasibility.
   Interested organisations are invited to join forces.
5. *Discussion and Conclusions*
   The discussion focused on:
   - Open Data in relation to user-controlled data and privacy.
   - The need to not only think about protecting data at its origin, but also at its use (e.g. by sticky policy)
   - But sticky policy delegates the problem to the HW, which creates strong need for data quality.
   - People are often creating the problems with security and privacy. This cannot be solved by technology only, but needs good governance.
   - There is a difference of data directly identitying or produced by the citizen/consumer on one side, and data coming from observation by third parties (e.g. service provider) on the other side. Ownership might be different.
   - We need a dialogue between people working on privacy and people working on forensics.