CPDP2011 - Panel on Privacy and trust in e-services

Privacy issues (Jacques Bus, Univ Luxembourg)

Given the short time and the intention to just make some statements, I would like to focus on some important issues, or call it complicating factors, that need to be considered when we talk on privacy technology in the field of ICT.

1. I do not believe in the **zero-sum game between privacy and security**. If any, there would be some balancing between security and freedom. Being safe and secure, means giving the same right to others, which of course restricts fully free action.
   Clearly, to make it win-win it needs a-priori thinking about privacy when designing a system for security: Privacy by Design; Systems and organisation that are transparent; and auditable behaviour of organisations (public or private).

2. Another important issue is, what has been made very clear by Helen Nissenbaum: **Privacy is normative and context dependent** (Contextual Informational Integrity).
   This must lead to assessment of privacy violations of new IT systems that takes these aspects (norms and context) into account. Nissenbaum gives in her latest book a framework for that.
   It does not mean that things should not change because our norms do not allow that, but that if things would violate our norms there must be a good and socially and ethically responsible reason for it, which is accepted by society through discussion and adapting its norms.

3. Mireille Hildebrandt uses a working definition for Privacy:
   'a reasonable measure of control of whether and to which extent one can be 'read' by what others in what context.'
   Inferencing through profiling by collecting info on Web behaviour, data mining, machine learning, location-based service, traffic monitoring, etc the definition of "personal information" or "personal identifiable information", i.e. the data subject to the Data Protection and Privacy regulations, becomes problematic. People and their behaviour can be constructed from a collection of data which all apart are not called Personal Information. And generally, even not connected directly to persons it can be used to forms of profiling that allows manipulation of people.
   Clearly to come to some solution of this we need trustworthy security of data storage by data controllers and we need data usage control by data subjects themselves. To allow them to build trustworthy trusted circles.

4. **Trust and privacy go hand-in-hand**: personal data is easier given to persons or organisations that are trusted. But that is not in the first place trust in technology. *Trustguide*, a project run by Cofta, LaCohee, and others concludes:
    a. Adoption of technical systems is not driven by trust in technologies, but by trust in the operators of such systems.
    b. People are aware that no security system is perfect and that over time, any identification system will eventually be compromised.
    c. In a citizen identity management system, government has an asymmetrically dominant role as an operator, which calls for very thorough consideration regarding the message of trust.

In general, privacy is about handling of data about or of persons according to accepted social norms, valid in a particular context. **It needs joint consideration of technology, social science, economics, ethics, law and other disciplines to bring us forward in this discussion.**

General context-independent data protection approaches and general models are important but not enough. Data that can and should be provided in one context, would be a breach of privacy in another. You want to give certain health data to your physician, but normally not to you bank or grocery.