[Conference - 2001 UbiComp] Privacy By Design (Principles of Privacy Aware Ubiquitous Systems)

This is a paper by Marc Langheinrich (ETH Zurich) which is one of the most cited papers in the domain. It was published at Ubicomp 2001.

The challenge is that:

- Computers are everywhere.

- Sensing equipment is more and more powerful, recording ait temperature to people's emotions.

- There is a huge memory capacity.

- Ubiquitous devices are not always visible.

The core principles are:

1 Notice.

Each device should "announce" the information it stores.

2. Choice and Consent

A subject should (be able to) give explicit consent to have information about hime saved.

3. Anonymity and Pseudonymity

Subjects do not have to be identifiable in all applications.

4. Proximity and Locality.

Implementing explicit consent means that every interaction potentially requires an explicit permission from a person. This is not very efficient. Proximity and locality are principles that make policies easier to specify. Proximity states that devices may store information about their owning subject so long as he is present. Locality states that devices may store information from devices in their neighbourhood, e.g., a house may store information from furniture.

5. Adequate Security.

Each device puts sufficient protection in place to protect information from inadvertant release.

6. Access and Recourse

Devices only store information for intended purpose and for no longer than needed.

The latter two principles reflect guidelines in the 1974 US Privacy Act and in the 1996 EU Directive 95/46/EC on the protection of individuals with regard to data processing of personal data and on the free movement of such data.