Since the bad guys will retain all data they can get anyway, the good guys probably are better off if they retain data as well

Andreas Pfitzmann
Technische Universität Dresden, Faculty of Computer Science, D-01062 Dresden
Nöthnitzer Str. 46, Room 3071
Phone: +49 351 463-38277, e-mail: pfitza@inf.tu-dresden.de, http://dud.inf.tu-dresden.de/

My Position: Forgetfulness

- Forgetfulness **cannot be reliably implemented in a distributed system** like the Internet. This is a show stopper: If *A* forgets, but *B* does not, this gives an advantage to *B*. So *A* would be stupid to let her computer forget in spite of *B* not doing the same with his computer.
- When we **discussed** forgetfulness in my group at Karlsruhe University **around 1986**, this complete lack of reliable implementability caused us not to write any line of text about it. Since then, my position did not change much.

My Position: Data Retention

- **Data retention** quite probably will be data retention **forever**. Probably not by the entities being entitled to access the data retained officially, like police or domestic secret services, and not by the telcos, either. But **by foreign secret services** and **organized crime**, getting to the retained data by hacking or social engineering.
- Of course, all officials will always tell us that the retained data are reliably erased as promised. And I even assume that most people telling us so really believe what they tell us.

Priorities

1. **Data avoidance**: Avoid that personal data can be gathered by others at all.

2. **Data minimization**: Minimize the amount of personal data and their sensitivity others can/do gather.
   User-specified expiration dates are *additional* sensitive data.

3. **Unlinkability**: Chunks of personal data should be unlinkable to other chunks.
   Implies that chunks do not contain too specific attribute values nor that chunks identify persons.

4. **Minimal spread**: The set of entities which ever get to know a chunk of personal data should be minimal.

5. **Minimal linkability**: The set of entities which ever can link different chunks of personal data should be minimal.
   Suggests that chunks do not contain too specific attribute values nor that chunks identify persons.

6. **Policies** how long to retain and how to use personal data should be agreed, and if possible, enforced.