Athens, 20/21 May 2014

Data Protection and IT Security after Snowden

Peter Schaar
European Acadamy for Freedom of Information and Data Protection, Berlin

What we know

- Publication of „Snowden-documents“ after 6/6/2013 by Guardian, Washington Post, NYT, Der Spiegel ...
- No official denial by US Government,
  but: declassified documents confirm many allegations
- Google, FB & Co.: „No direct NSA access to our servers“
  but: Co-operation on basis of legal requirements confirmed
- CALEA requires telcos to provide law enforcement authorities and secret services with technical means for surveillance, not (yet) applicable to Internet services (CALEA II ?)
- Co-operation agreements still confidential? Provision of technical interfaces beyond legal requirements?
- Secret NSA access on internal networks of Google, Microsoft ...
- Targeted access operations on specific networks, persons, computers, industries …

Programs

- Prism
- Tempora
- X-Keyscore
- Bullrun
- Muscular
- ….

Challenges

- Globalised data
  - Ubiquitous collection and processing
  - Global transfer within milliseconds
  - Massive collection of Metadata „by the way“
- National protection
  - territorial limitation of data protection legislation
  - exterritorial application of national law? (FISA-requests …)
  - different understanding of legal terms (secrecy of telecommunications, data protection, privacy …)
  - Different standards for own citizens and foreigners
  - Lack of enforceability outside the own country

Answers

- **Legislation**
  - International law (United Nations … Civil Rights Covenant, CoE ...)
  - European Union
    - ECJ judgements on Data Retention / Google Spain
    - Data Protection Reform package (regulation+directive)
    - Non disclosure provision (Art. 43a)
  - „No spy“ agreements? - no spy guarantees !
- **Technology**
  - Routing/Hosting requirements („Schengen Routing“?)
  - Anonymous use/ pseudonyms
  - Encryption