Caspar Bowden
(independent privacy advocate)

Data Protection for the Digital Age

Greens/EFA hearing

28 June 2012

Conceptual flaws in DP

- (~1975) predates PCs, Internet, crypto, SNS
  - "technological neutrality"

  = DPAs don't have to understand technology ?
- unreal legalistic concept of privacy risk
  - many copies of data OK if legal control?
  - ..but obviously increases threats to privacy
  - legal fiction that "free-flow" & privacy compatible
- "anonymous" data now easy to re-identify
  - what is "personal" ? Identifiable by whom?
  - better for privacy not to store data at all
  - but DP has same rules for all "processing" ?!

Privacy Engineering

- "data minimization" is good..
  - but also need minimize privacy risk
  - litmus test: risks to subject same before/after?
- PETs are magic: have cake and eat it
  - e.g. authentication without identification
  - "anonymization" of data mostly nonsense
  - ...but anonymous system design is possible
  - Problem: DPAs think PETs pre-empt their role!
- Usable PETs are hard to design
  - for Controllers: more data = more profit
  - how incentivize (non-EU) "big software" ?

Foreign Intelligence Surveillance Amendment Act 2008 **1881(a)**

"Procedures for targeting certain persons **outside the United States <u>other than</u> US persons**"

- **"foreign intelligence information"** (concerning **non-US persons**)
  - information with respect to a **foreign power** or **foreign territory** that **relates** to the conduct of the **foreign affairs** of the United States
  - serious crime, nat.sec. economic intel. NOT REQUIRED

- **"foreign power"**
  - a **foreign-based political organization**, not substantially composed of United States persons

- **"remote computing services"**
  - provision to the public of **computer storage or processing services** by means of an **electronic communications** system

=> US Cloud providers can be forced secretly to allow NSA inside the datacentre and/or put backdoors in software for **purely political mass-surveillance**

Transborder “derogations”

- general problem of contracts/legal “control”
  - moral hazard for controllers/processors
  - laws unenforceable-by-design for subjects
- BCRs-for-processors
  - vacuous-by-design, concocted for Cloud
  - are Cloud providers “merely” processors?
- “Safe Harbor-for-processors” ?
    - => all SHA Principles become void !
      - SHA self-certs by big Cloud vendors
  - EU and US played “chicken” : EU lost
  - DPAs say “not our problem”; Commission ?

Conclusions

- US Cloud mass-surveillance already legislated in 2008 (FISAA 1881a)
- FISA vs. ECHR: no NONUSPER rights
- DPAs no legal competence for FISA; no technical competence in comp.sci
- Cloud cannot be “audited”
  - real Cloud is not “hosting”
  - “audit” means not DPAs problem
- must close “the Cloud loophole”
  - else all other DP safeguards FAIL