Privacy and surveillance on the Internet
What happened, and what to expect next...

Caspar Bowden

independent privacy advocate

(formerly: Chief Privacy Adviser, Microsoft Europe
Director, Foundation for Information Policy Research, www.fipr.org)

Panoptykon – Internet at the Crossroads

Warsaw 20th September 2011

Review of Data Protection Directive

"official" agenda

- Principle of "Accountability"
- Right to be Forgotten
- *faux* "Privacy by Design"
- Privacy by Default (?)
- "flexible" export rules
- DPA forum shopping (aka "harmonization")

the real privacy agenda

- "anonymisation"
- right to online access
- Privacy engineering
- Data minimization
- Art.29 fails to enforce against major Internet companies
- future of Safe Harbor ?
- DPA computer science competence ?

Anonymization is a legal fiction*

- DPD exempts “anonymized” data from regulation
- ….but what do we mean by anonymous ?
  - external “auxiliary” data, “intersection attacks”
  - Shmatikov 2008 Netflix paper + algorithm
  - social network relationships cannot be anonymised
    - Dwork 2008 – “structural steganography”
- Paul Ohm’s paper “Broken Promises…”
- *Transparent Government, not Transparent citizens (Ch.4 2011 UK report, Dr.Kieron O’Hara)
  - *“the EU Directive forbids the release of almost everything, while the UK Act, which supposedly implements it, will allow rampant reidentification!”*

The problem of "personal" data: "identifiable" by whom ?

- DPD split definition of personal data between an Article and Recital 26
  - Recital 26 has crucial 5 words "or by any other person"
  - …but because a Recital, not mandatory to transpose !
  - …the most important term of DP art was crippled at birth in 1995
- UK and IE are "leaky buckets" : export pseudonymous data with impunity.
  - How did UK allow 1 month of all UK telephone records to go to US ?
    - Each telephone number replaced with a random number, but social structure remained intact! Biggest privacy breach from any EU country ?
  - massive EU internal market **regulatory arbitrage**
- Question: if DPAs have ruled that passport#, credit card#, tel# are personal, why not IP addresses, cookies, MACs?
  - Answer: because DPAs took ten years to understand what an IP address was!
  - Art.29 Opinion "concept of personal data" : 25 pages to explain 2 paragraphs!

The really simple version of why Safe Harbor doesn't cover Cloud

- suppose you and I make a deal which depends on agreeing to respect a handful of principles.
- In some obvious and forseeable situation, it is impossible to give effect to any of the principles, causing serious risk and detriment to me.
- Is it fair to assume our deal was intended to include this situation ?

What would mass-surveillance of Cloud Computing look like?

- dig up road outside big data centre
- tap the fibre-optic cable
- shunt data to equally big data centre for triage and analysis

But surely all the data going in and out will be encrypted (and some big service providers were “persuaded” by activists into switching on encryption by default)

Even the Patriot Act can’t make US companies give up decryption keys like that funny UK law (RIPA 2000 Pt.3)

Well, (don’t entirely forget about Patriot, but)

Have you ever heard of……

FISA Amendment Act 2008

- Scandal of “warrantless wiretapping”: 2005-2008
  - AT&T technician discovered much US Internet traffic being tapped, triaged, diverted to National Security Agency
  - FISA 1978 required “minimization” of intrusion on US persons
  - To and fro saga of US Administration officials being kept in dark, refusing to re-authorize “Terrorist Surveillance” programs
- FISA Court had rejected major authorization circa 2005: President of Court withheld facts from other judges (!)
  - substance of argument about how hard NSA had to work to prevent collection of data of “U.S. persons”
  - Protect America Act changed to doctrine of minimize-use-not-collection. FISA Court now “approves” policy of ODNI
- **FISAAA 2008 s.1881 authorizes political surveillance of non-US persons outside US, and expressly includes Cloud Computing ("remote computing services“)**

summary

- Data Protection
- Anonymization
- Cloud Computing
- EU/US “Safe Harbor” “Agreement”
- Internet mass-surveillance and Fundamental Rights
- ….is it all a question of “balance” ?

Conclusions

1. Privacy engineers need a precise definition of personal data so they can minimize what they collect, protect what they process, and give the user access to their own data safely and privately. Unless regulators apply clear, consistent and forceful pressure to innovate in privacy technology, vested interests will suppress
2. Clarify to the US that Safe Harbor is not applicable to Cloud Computing. Create new central authority for EU transnational enforcement
3. DPAs should employ (many) more post-grad engineers in privacy computer science (viz. salutory effects on FTC 2009-)
   - "technological neutrality" does not mean "if it's technical, DPAs don't need to understand it" !
4. if the right of subject access is to be useful, people need a legal right to access their data online (at least if the "service" is online)

Recommended reading

"Online Privacy: Towards Informational Self-Determination on the Internet"

(Dagstuhl Perspectives Workshop 2011)