Open problems in applying PETs to EU Data Protection

Torys LLP Technology Law Series

26.10.2004

Caspar Bowden
Chief Privacy Advisor
Microsoft EMEA Technology Office

The human right to privacy

– European Convention on Human Rights (1950)
  - ECHR rulings are binding in 45 signatory states

– Data Protection Directives (1995, 2002)
  - binding on member states
  - 25 EU + 4 EFTA
  - establishes legal rights of data subject
  - independent national DP authorities
  - Art.29 Working Party

– EU Charter of Fundamental Rights (2000)
  - explicitly includes Data Protection
  - binding on EU institutions
  - EU Data Protection Supervisor

EU Data Protection concepts

DP principles for Personal Data (identified/identifiable)

- processed fairly and lawfully
- collected and used for specified purposes
- relevant and not excessive in relation to purpose
- accurate and up to date
- rectified if found incorrect
- not retained longer than necessary
- protected with appropriate organisational and technical security measures
- transfers outside EU are controlled

Data subjects

- Can require controllers to provide snapshot of all personal data

  (“subject access”)

‘Sensitive’ data

- ethnicity, politics, religion, sexuality, health, trade union membership, criminal records
- explicit freely-given consent

Data controllers

- register purposes, ensure compliance
- respond to ‘Subject Access Requests’ within fixed time for flat fee

Data processors

- Process data on behalf of controllers
- Do not decide purposes of processing

Art.29 Working Party

- Article.29 Working Party
  - Committee established by 1995 Directive, comprising national DPAs
  - advises EC on implementation, harmonization
  - “soft-law” Opinions influence national interpretation

- …some notable Opinions
  - Integrated approach to Internet privacy [WP 37]
  - IPv6 use of unique identifiers [WP 58]
  - Safe Harbor [WP 31/32/62]
  - Applicable law for non-EU based web sites [WP 56]
  - Minimum requirement for on-line data collection [WP 43]
  - On-line authentication (Passport/Liberty) [WP 60/68]
  - Binding corporate rules on international transfers [WP 74]
  - E-Government [WP 73]
  - Biometrics [WP 80]
  - Trusted Computing Platforms [WP 86]

Privacy Enhancing Technologies (PETs)

- Microsoft's Trustworthy Computing initiative :
  - *privacy means the ability of individuals to control data about themselves, and adherence to fair information principles*.
- Privacy can be infringed when (without informed consent) records are disclosed **or** behaviour is profiled
  - whenever individuals use computer services, logs may be kept indicating who they are, where they are, and what they do.

- Privacy Enhancing Technologies can allow the user to control how much they can be profiled
  - Consumer and citizen concern increasing
  - "Nothing to hide, nothing to fear" ?
  - Is there *something* you would legitimately prefer *someone* not to know ?

- Privacy Engineering – integrating privacy by design
  - identifiable data at network vs. application layer
  - minimisation for purpose
  - advanced PETs for privacy with security

EU Commission stance on PETs

Promotion and encouragement of Privacy Enhancing Technologies

- *"…The concept of privacy enhancing technologies is **already an integral part of the Directive** but …**necessary to take additional measures** to promote the use of these technologies."*
- *"…to design information and communication systems and technologies in a way that **minimises the collection and use of personal data** and **hinders unlawful forms of processing…use** of appropriate technological measures is an essential complement to legal means and should be an integral part in any efforts to achieve a sufficient level of privacy protection. Technological **products should be in all cases developed in compliance** with the applicable data protection rules."*
- *"…the difficulty of **recognising which products are genuinely PETs**...some systems presenting themselves as PETs are not even privacy-compliant."*
- *"…The key-issue is therefore not only how to **create technologies that are really privacy enhancing**, but how to make sure that these technologies are **properly identified and recognised as such by the users**.*
- *"…The objective is not just better privacy practices, but also to **increase transparency and therefore the trust of users** and to give those investing in compliance and even enhanced protection an opportunity to **demonstrate their performance** in this respect and **exploit this to their competitive advantage**."*

- EU Commission Report on the implementation of the DP Directive (15.5.03)

Types of PETs

- Anonymity/Unobservability
  - Infrastructure: network layer
  - Onion-routing, MIXes, Crowds, PIR
- Pseudonymity/Unlinkability
  - Credentials : application layer
    - authentication without identification
    - control linkability of transactions
    - conditional anonymity
      - derived from e-cash ‘double-spending’ ideas
- “Data Governance”
  - privacy rights management languages to express and enforce policies for identifiable data
  - towards enforceable privacy preferences?

Privacy Risks - data controllers

- Liability: Sanctions, Reputation, Damages
  - Unnecessary collection
  - Improper use or disclosure
  - Excessive retention – type or time
  - Insufficient organisational or technical security
  - Incomplete or incorrect SAR fulfilment
    - negligent authentication or delivery
  - civil litigation

Privacy Risks – data subjects

- Incomplete access
  - lack of forseeability, self-determination
- Obscure or ambiguous notices
  - definitions of “identifiable” vs. “anonymous”
  - time cost of scrutiny exceeds marginal value
    - unappreciated consequences
- Declared policy not observed/enforced
  - unrecognised data flows
  - ineffective controls on data processors

Subject Access

- Transparency
  - …but two-thirds EU citizens unaware of right!
    - EU Eurobarometer survey 2004
- Authentication
  - Who is the data subject ?
  - Identity Management
    - Privacy risk of making scattered data easier to collate vs. benefit of making SAR easier to fulfill
- Fulfilment
  - Where is the data ?
  - Redaction of references to other persons
  - Secure delivery online – what will suffice ?

Subject Access Requests

- Authentication
  - is the requester the data subject?
    - risk of improper disclosure
      - Privacy threat models
        - » User's point-of-view that matters
        - » Wide spectrum of user sensitivities, individual threat models
      - social engineering, authorised insiders
- Where is the data?
  - Archives (e-mail, server, database, offline)
  - Scattered over different desktops, caching

Disproportionate effort “exemption” for Subject Access?

- UK DPA 1998 – need not provide data in “permanent form” if would require disproportionate effort
  - 2002 UK consultation – ***“It is important to note that the personal data must always be provided. The ‘disproportionate effort’ test applies only to the way in which access is given.”***
    - Lord Chancellor's Department Consultation Paper, Data Protection Act 1998: Subject Access, October 2002
      - Permanent form = hard copy
- often data controllers interpret in practice as a general exemption
- Enterprise ID Management systems could have the effect of broadening regulator expectations of reasonable fulfilment of access requests
- …but Durant vs. FSA (2003) narrowed scope?
  - …but EU Commission dissatisfied with UK transposition (2004)?

Data lifecycle in the Enterprise

- Conflicts between retention/deletion rules
  - DP minimisation/deletion principles still apply to sectoral retention requirements
  - typically context dependent and ill-defined
    - too complex/unclear/expensive to automate?
- When are identifiable audit trails justifiable?
  - Minimally intrusive for necessary effectiveness
    - weigh security needs against privacy risks
    - deterrence of abuse needs visible policing
    - logs of usage data are personal data too!

Pseudonymous Subject Access?

- Data controller may only know subject pseudonymously (*are* they a “controller” ?)
- 1995 EU DP Directive defines “personal data” as:
  - “any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, **directly or indirectly**, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, **cultural or social** identity”
- Is data related to the pseudonym eligible for subject access?
- Should the data subject be required to disclose real-world identity to access?
  - Example: handle in a newsgroup/chatroom - traceable via IP/cookie?

Q&A

Caspar Bowden - casparb@microsoft.com
http://www.microsoft.com/twc
Chief Privacy Advisor
Microsoft EMEA Technology Office