Does the cloud require a new privacy framework?

The European perspective

Thomas Fetzer
1. The foundations of privacy rights in Europe
   1. The theoretical foundations
   2. The Data Protection Directives

2. Application of the current privacy framework to cloud computing
   1. Jurisdiction
   2. Responsibility
   3. Selected relevant obligations for cloud computing

3. Does the cloud require a new privacy framework?

4. Outlook
1. The foundations of privacy rights

• The right to the protection of personal data is rooted in the fundamental right to personal self-determination ("informational self-determination")
  – In Germany privacy rights are also based on Art. 1 GG ("human dignity") which is at the apex of the German constitution
  – Art. 8 Charter of Fundamental Rights of the European Union

• Core principle: Individuals must be able to control their personal data at any time
  – Personal data must not be processed without either the consent of the individual or an explicit statutory permission
  – The government must not intrude into the privacy of individuals AND it has a duty to protect the personal data of individuals against intrusion by other private parties
1. The foundations of privacy right

- Based on these theoretical foundations the privacy framework has been harmonized by European Directives
  - Directive 95/46/EC on the protection of individuals with regard to the processing of personal data of 1995(!)
    - Applies to “personal data” = any information relating to a natural person
  - Directive 2002/58/EC on privacy and electronic communication
    - Applies only to telecommunications data (e.g. traffic data)
  - Directive 2006/24/EC on the retention of telecommunications data
    - Applies only to telecommunication data (e.g. traffic data, location data)
2. Application of the current privacy framework to cloud computing – Jurisdiction

**Generally**

- **Principle of territoriality** (Art. 4 Directive 95/46/EC)
- EU law applies if the *processing* of personal data takes place within the EU
  - The controller is established within the EU and it processes personal data within in the EU
  - The controller is established outside the EU but uses IT infrastructure within the EU
  - Personal data is transferred (=processed) to a third country

**Application to cloud computing**

- EU law
  - Applies to “European clouds”
  - Does not apply to “Third-country-clouds”
  - Multinational clouds???

**Problem**

- Creates legal uncertainty for cloud providers
- Leaves room for “jurisdictional arbitrage” at the expense of individuals
2. Application of the current privacy framework to cloud computing – Responsibility

Art. 6 par. 2 Directive 95/46/EC

*It shall be for the controller to ensure that the obligations constituted by the Directive are complied with.*

Art. 2 lit. d) and e) Directive 95/46/EC

*“Controller” shall mean the legal person which determines the purposes and means of the processing of the personal data.*

*“Processor” shall mean the legal person which processes personal data on behalf of the controller.*

**Article 29 Data Protection Working Party**
**Opinion 1/2010 of 16 February 2010**
2. Application of the current privacy framework to cloud computing – Obligations

Generally

- **Data security**, Art. 17 par. 2 Directive 95/46/EC
  - Controller must ensure that the processor provides for appropriate technical and organizational measures to protect personal data
  - It must be guaranteed that the processor acts only on instruction from the controller

Application to cloud computing

- Company that uses service of a cloud provider must ensure that the cloud provider
  - provides for appropriate technical and organizational measures for its entire IT to protect personal data
  - acts only on instructions from the client

Problem

- How should a cloud user be able to ensure this if it is not necessarily predictable what infrastructure is used and where it is located?
2. Application of the current privacy framework to cloud computing – Obligations

Generally
- **Transfer of data to third countries**, Art. 25 par. 1 Directive 95/46/EC
  - Personal data must not be transferred to third countries that do not ensure an adequate level of protection

Application to cloud computing
- The transfer of personal data within a „European cloud“ is possible
- Transfer of personal data within a „Third-country-cloud“?

Problem
- Creates a high level of uncertainty for “Third-country-clouds”
- Data Protection Officer of Berlin just recently issued a report stating that it violates the German Data Protection statute to use “Third-country-clouds” without explicit consent of the individuals to whom personal data belongs *(Data Protection Officer of Berlin, Datenschutz und Informationsfreiheit Bericht 2008, p. 18)*
3. Does the cloud require a new privacy framework?

European privacy principles and cloud computing are not compatible

Cloud computing needs – at least in Europe – a new privacy framework

Harmonization in Europe is not sufficient to create legal certainty

Global efforts? Cyber Crime Convention?
3. Does the cloud require a new privacy framework?

- Privacy rights are of paramount importance in Europe (especially in Germany) and there is a duty for the government to protect privacy rights in the Internet world.
- However, the current privacy instruments which are based on the core principle that individuals must be able to control their personal data at any time might no longer be well-suited.
- A new framework could be based on more market-based instruments.

➢ User information as a prerequisite for personal self-determination.
4. Outlook

- The protection of privacy rights is constitutionally enshrined in the Constitutions of many Member States
- The German Constitutional Court has frequently demonstrated its determination to apply the core principles – that individuals must be able to control over their personal data at any time – without exemption to the Internet world
  - BVerfG, Decision of 27 February, Docket No. 1 BvR 370/07
    - The right to informational self-determination includes a right to privacy and integrity of electronic information systems
    - The right to informational self-determination must be strictly applied to new technologies
  - BVerfG, Decision of 2 March 2010, Docket No. 1 BvR 256&263&586/08
    - A telecommunications data retention for six months violates the constitutional privacy rights (Art. 10 GG – privacy of telecommunications)
    - Germany still has the authority and the obligation to protect privacy rights if the EU does not provide for a sufficient level of protection
4. Outlook

Efficient cloud computing under the current legal framework – almost impossible!

A new privacy framework for the cloud – mission impossible?

Thank you for your attention!

Priv.-Doz. Dr. Thomas Fetzer, LL.M. (Vanderbilt)
University of Mannheim School of Law and Economics
Mannheim, Germany
fetzer@uni-mannheim.de