To cloud or not to cloud, that is a very serious question…

EEMA / TrustCore

Legal challenges in a post-Safe Harbour and pre-GDPR cloud world

18 November 2015
hans.graux@timelex.eu

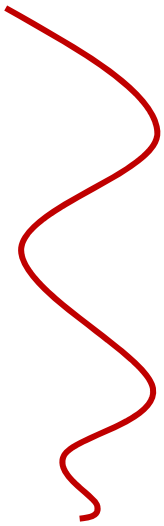
Context

- Major cloud providers are predominantly “American”
- Snowden-revelations ⇔ American law ⇔EU law
- (Personal) data in the cloud?

Major players (IaaS) – Gartner Magic Quadrant 2015

- Amazon AWS
- Microsoft Azure
- Rackspace
- CenturyLink
- Google Cloud Platform

The red threads on cloud in the EU…



We love cloud computing, and fully endorse it!

- We want some of that market
- We want those benefits

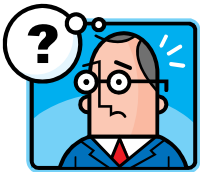
Our fundamental rights are non-negotiable!

- Privacy and data protection are human rights
- They need to be clearly protected

But maybe we shouldn't be fully dependent on foreign undertakings

- Concerns about vendor lock-in, monopoly abuse, stability
- And what about market share and jobs…?

So what about this data protection stuff in the cloud?



- EU data protection law
  - Now: Data Protection Directive 95/46/EC
  - Applies when "processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State"
- Near future: General Data Protection Regulation
  - Near future: General Data Protection Regulation
  - Now: General Approach - http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf
  - Same applicability rule, and also "to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to:
    - (a) the offering of goods or services, irrespective of whether a payment by the data subject is required, to such data subjects in the Union; or
    - (b) the monitoring of their behaviour as far as their behaviour takes place within the European Union"

So European data protection law applies!

And our privacy is effectively protected. All is well.

Except maybe in some cases…

- Executive Order 12333 – 1981
  - Attorney General may seize foreign intelligence
- Foreign Intelligence Surveillance Act (FISA) - 1978
  - Attorney-General and Director of Foreign Intelligence may demand electronic communication service providers for cooperation on foreign intelligence information.
- Electronic Communications Privacy Act (ECPA) – 1986
  - More similar to European criminal law instruments

Legal protections for EU citizens?

- No data location criterion
- No individual target required
- No systematic independent judicial revies
- No opportunity of redress
- Fourth Amendment is for US citizens only
- A systematic link with the United States is sufficient

Enter Max Schrems and Facebook

- Legal debate was on cross border data transfers
- Within the EU/EEA? No problem (as long as all principles and rules are adhered to, of course).
- To third countries? Forbidden, unless:
  - Adequate countries (mainly Canada, Switzerland, Israel, Argentina, New Zealand, and Uruguay)
  - ~~Safe Harbor~~
  - Model Contracts – Standard Contractual Clauses
  - Binding Corporate Rules
  - Exceptions: consent, necessity of various kinds.

Safe Harbor

- Only for the USA
- A framework of principles, negotiated between the EU and the USA, in which US based companies can self-certify their compliance
- Approved by Commission Decision 2000/520/EC
- List of Safe Harbor compliant companies is managed and published by Export.gov
- Includes many large US companies, including Facebook Ltd.

Things you should know about Max Schrems

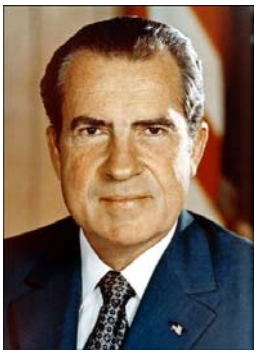
- Austrian student
- Facebook member since 2008
- Unhappy about mass surveillance, and willing to go to court over it
- Went to the Irish Data Protection Commissioner, who refused due to (1) lack of evidence and (2) the Safe Harbor
- Went to the Irish High Court, who referred it to the European Court of Justice
- Safe Harbor decision on 6 October 2015. Court of Justice replied that:
  - DPAs could still assess any data transfers, including those within a Commission Decisions such as the Safe Harbor
  - More specifically, the Safe Harbor Decision, in the light of the Snowden revelations, could no longer be considered as valid.
- In effect, the Court of Justice annulled the Safe Harbor framework through its decision.

So is the cloud now officially dead in Europe?

- Not quite
- Safe Harbor is gone now, but:
  - Other transfer mechanisms are still available
  - Safe Harbor 2 negotiations were already ongoing and speeding up
  - The GDPR is still coming along
- What we do have, is mass concern and reluctance.

Ethically ambiguous and politically inconsistent

- Isn't the data protection issue *largely unrelated* to the Safe Harbor…?
- Isn't the bigger concern *largely unrelated* to data protection…?
- Doesn't *every country* have far reaching national security laws…?
- Aren't we *all* refusing to sit around the table to come to a consensus on these issues…?



The GDPR – what it will and will not fix

- Anticipated in the next few months
- Will put in place a single data protection law across the EU
- Will strengthen (among other points) security/operational requirements, third party certification, and enforcement (liability and fines – max. 1 million or 2% of worldwide turnover)
- Will not harmonise national enforcement
- Will not touch on national security

So what can be done to save the cloud from policy issues?

- 'Easy' fixes: GDPR and Safe Harbor 2
- Doable: reciprocity in enforcement – redress between the EU and US
- Probably not doable: alignment on the need for proportionality – legitimacy – independent supervision at the international level
- Probably more realistic: better technical measures – (homomorphic) encryption

Questions and comments?

Hans Graux
(m) 0032 (0)479 79 55 00
(e) hans.graux@timelex.eu

time.lex
Rue du Congrès | Congresstraat 35
B-1000 Brussels

(t) +32 (0)2 229 19 47
(f) +32 (0)2 218 31 41

info@timelex.eu
www.timelex.eu

time.lex