Privacy by Design: How to Translate Privacy Law Provisions into Technical solutions

IAPP – Global Privacy Summit
Washington DC
March 9-11, 2011

Francesca Gaudino, Senior Associate, Baker & McKenzie
Jan Seedorf, Senior Researcher, NEC Laboratories Europe

© 2011 Baker & McKenzie
Outline

- Risks and benefits of new technologies
- From PET to Privacy by Design
- The need of interaction between technology and law
- DEMONS Project
- Some practical examples of transposition of legal concepts in technical solutions
Technology: good or bad guy?

- Cutting edge technologies make life easier
- Information never before so available
- Consumer as ‘prosumer’ of content and products
- Ubiquitous solutions make the ‘global village’
- Rich staffed menu of on demand services
The dark side

- Trade off between privacy and technology
- The right to be forgotten
- Global village is too ‘global’
- Excessive encroaching in private lives
- “Personal data is [...] the currency of the digital world”
- Unlike love, online is forever
The right perspective

- Technology simply performs according to the planned results
- Design of technology from the very initial stage with in mind regulatory issues
- Access control policies, logging functionalities, semantic solutions, pseudonymization, encryption features
- Translation of law provisions into technical solutions
- Enforcement is the hardest goal in digital world
PET vs Privacy by Design

- PET was more concerned with ‘privacy-aware functionalities’ applied to existing technologies
- Privacy by Design fosters building privacy preserving technologies
- FTC: a somehow different approach
  - company privacy practices
  - data management procedures
Technology and Law

Not always an easy relationship…

- If you’re a lawyer
  - need some command at technicalities
  - learn the jargon!
  - admit you’re hopeless…

- If you’re a technician
  - accept the concept of ‘interpretation’
  - learn to think in *general terms*
  - be patient
How it works in practice

But it can work!

- Identify scenarios
- Draw a clear regulatory framework as fixed border
- Translate the law into the practical result
- Plan the technology architecture and choose implementation solutions
- Flexibility is of essence (localization, new laws, new business needs, new technology threats)
The Regulatory Assessment

- Identification of use cases
- List the regulatory requirements – EU legislation plus national peculiarities
- Find a benchmark: EuroPrise (European Privacy Seal) Criteria Catalogue
- Privacy Matrix as metric/testing procedure to assess legal compliance of a given technology
The privacy matrix is organized in five fields:

- regulatory provisions
  - descriptive comments: results to be achieved
- technical functionality for the relevant provisions
  - technical comments: details of the solutions and possibly their functioning
- assessment result: Yes / No / Not applicable

Each regulatory provision is assessed against specific functionalities and solutions of the system.
Consortium

Project Coordinator: TID
Status: Negotiation Phase (deadline: April 7th)
Total Budget: 9M €
Target EU Funding: 5,35M € Max.
Expected Start: Summer 2010

Telefónica I+D
NEC Europe
CNIT
France Telecom
Institut Telecom
ETH Zürich
FTW
INVEA Tech
Telekomunikacja Polska
Singular Logic
Telscom AG
Optenet
Today’s monitoring systems

- Centralized
- Huge amount of exported/collected data
- Hard/no cooperation across domains
- Poor flexibility in access control to monitored data (little more than Y/N)

Hardly coping with
- Higher link rates and traffic volumes
- Networks pervasiveness & capillarity
- distributed, cross-domain, threats
DEMONS: Vision

Overlay of in-network monitoring devices
From data-gathering probes to **collaborative P2P computing and filtering devices**

<table>
<thead>
<tr>
<th>Innovation pillars</th>
<th>Target Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>In-network processing and distributed intelligence</td>
<td>Scalability</td>
</tr>
<tr>
<td>Application-tailored data reduction and protection</td>
<td>Privacy preservation</td>
</tr>
<tr>
<td>Resilient autonomic monitoring overlay</td>
<td>Flexibility and resilience</td>
</tr>
<tr>
<td>Cross-domain interworking</td>
<td>Cross-domain threat detection and mitigation</td>
</tr>
</tbody>
</table>

**Exchange only the information strictly necessary for a given monitoring and analysis objective**
Multi-domain picture

Caption:
- Local DEMONS deployment
- Local probe, status normal
- Local probe, status alarm

Individually, this probe belonging to TE is detecting several customers performing anomalous HTTP connections to a server outside EU

An application running at FT correlates that anomalous HTTP connections at TE and TP are part of a DoS performed by bots

Individually, this probe belonging to TP is detecting several customers performing anomalous HTTP connections to a server outside EU
DEMONS: Technical Approach

Application Layer
- Cooperative applications
- Application adaptation and deployment
- Presentation & visualization

Coordination Layer
- Resilient, scalable monitoring overlay
- Orchestration, authorization and control of distributed operation
- Inter-domain cooperation

Measurement Layer
- In-probe processing and filtering
- Composable traffic analysis tasks
- Flexible & programmable devices
Privacy-by-Design in DEMONS

• Full involvement of privacy experts from the start
  – privacy experts participate in all project meetings during the technical design phase of the project, and provide critical input to technical discussions from a legal compliance perspective
  – acting not simply as advisors, but as project partners who influence decisions

• Specific tasks for privacy analysis in work plan
  – looking for privacy and regulatory constrains applicable to the DEMONS architecture at all layers
  – providing results/input to requirements and architecture tasks

• Technical workpackage on privacy preservation techniques
  – ensuring that the privacy considerations which have been identified are addressed with technical solutions
Our experience ...

• Communication between legal experts and technicians can be cumbersome at times
  – Legal constraints are often perceived as an unnecessary hindrance by technicians
  – Advice from privacy experts on legal compliance is sometimes misunderstood as “blocking technical progress”

• Early involvement is crucial
  – In several occasions, legal perspective was key to correct technical design at early stage

• Don’t underestimate effort for privacy by design
  – Collaboration between legal experts and technicians needs lenience from both sides, this may take time
Practical tips for interacting with technicians

– **Early involvement**
  - Absolutely key to the concept of Privacy-by-Design
  - The earlier privacy issues are precisely identified, the more time technicians have to develop corresponding technical approaches

– **Be aware of how technicians look at legal constraints**
  - Be sensitive to this conception, try not to be perceived as arrogant

– **Plan sufficient effort for Privacy-by-Design**
  - Collaboration and establishing mutual respect may take time
  - You may not be welcome at first ...
Practical tips for interacting with technicians

– **Speak in non-legal terms**
  - Explain the situation in non-expert terms as much as possible, otherwise you risk that technicians get bored or misunderstand

– **Aim for collaboration instead of conflict**
  - Try to establish an atmosphere of collaboration and mutual respect rather than being recognized as an “adversary“ who stops innovation
  - If possible, socialize with technicians

– **Be constructive!**
  - Avoid saying: “not possible at all“
  - Offer alternatives, actively help to adapt/design technical proposals
Shopping List

- Identify the output of your technology
- Select the real scenario for implementation
- Draw the legal framework, peculiarities included
- Translate the law into technical language
- Merge the legal and technical requirements
- Perform the regulatory assessment
- Review the requirements and update the assessment regularly
References

- Directive 96/46/EC; O.J. L 281, 23 November 1995
Acknowledgement

• This work was partially supported by DEMONS, a research project supported by the European Commission under its 7th Framework Program (contract no. 257315). The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the DEMONS project or the European Commission.
Questions???

francesca.gaudino@bakermckenzie.com
jan.seedorf@neclab.eu