Legal implications of network monitoring:

privacy threats and requirements

Francesca Gaudino
Baker & McKenzie Milan - Italy
francesca.gaudino@bakernet.com

Scope of the presentation

- Privacy threats in network monitoring
- Application of privacy legislation to network monitoring
- Brief highlight of solutions adopted by PRISM

Privacy threats over the Internet

Internet = *Privacy Killer:* published data are virtually

out of control

disclosed to ‘anyone’

forever online (the right to be forgotten)

Privacy threats in network monitoring

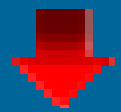
Network monitoring is necessary and in principle legitimate

BUT

- It allows monitoring of users' activities and communications
- It allows the gathering of a massive amount of data
- User is often unaware of the data collection
- Security breaches
- Abuse of data and users' profiling

Privacy legislation in network monitoring

Does privacy legislation apply to network monitoring???



Privacy legislation rules on the *processing* of *personal data*

Privacy legislation in network monitoring - 2

- Processing is any kind of operation performed on data, including mere reading

- The concept of INDIRECT IDENTIFICATION DATA: a person identifiable indirectly through association with other information

  - any information

  - possessed by any third party

Key coded and anonymous data

- Art. 29 Working Party; Opinion 4/2007 on the concept of ‘personal data’
- Key coded data are indirect identification data
- Anonymous data only when anonymization is complete and irreversible
- Anonymous data are personal data before being rendered in anonymous form
- IP address (static and dynamic) is a personal data

Application of privacy legislation

- Who is the data Controller???

The data Controller is who decides the purposes and conditions of the processing, including security issues

- What is the applicable privacy law???

It should be applied the national privacy law of the place where the data Controller is established

Privacy requirements – The data subjects

The main privacy requirements to be considered towards the data subjects (users):

 information (consent)  privacy rights

- Users should be made aware that their data are processed and of the processing purposes, conditions and extent of data communication

- Users should be enabled to excercise their privacy rights to actively intervene in the processing of their data

Privacy requirements – Third Parties

- National Data Protection Authorities (notification, filings)
- Third parties involved (service providers) and/or data recipients: necessary contractual measures or other arrangements to guarantee a lawful processing
- Data security measures to protect data in the static and dynamic phases of the processing, against external and internal intruders

Exemptions may apply

- The processing purpose may offer some exemptions (e.g. information and consent)

Research, study, analysis purposes

- Data quality ('anonymization') and purpose sought may offer lower severity in application or exemption

Data reversion very difficult and identification out of the scope of the data processing

<u>To be considered on a case-by-case basis and under national applicable privacy law</u>

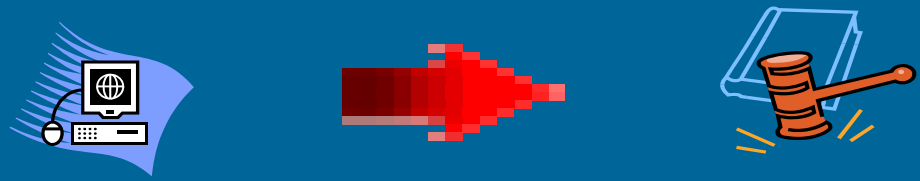
Further privacy issues to be considered

The transfer of data out of EU

Specific precautions to protect the transferred data

- Safe Harbor for US based recipients
- Data transfer agreement (EU Model Clauses)
- Binding Corporate Rules for group of companies
- Consent of the data subjects (secondary solution)
- Specific authorization of national DPA
- Others according to national applicable privacy law

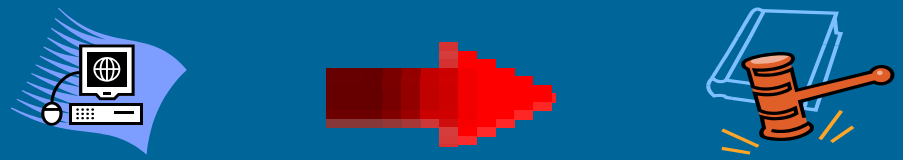
Techical concepts into law provisions



Italian privacy regulation on storage and processing of telephone and telematic traffic data

- January/July 2008; April 2009 extended to December 2009
- Strong and biometric authentication to access data
- Access record system; deletion procedures
- Encryption in storage
- Strong segregation for technical functions and IT systems

Techical concepts into law provisions 2



Italian Regulation on system administrators: November 2008; June 2009 extended to December 2009 with FAQ

- Who controls the controller??? Experience, skill and reliability
- Extensive definition of ‘system administrator’
- Audit log (timestamps and event descriptions) for 6 months
- Annual checks
- Disclosure to employees

PRISM privacy compliance solutions

Two tier architecture

- Front-end: at the traffic probe device to guarantee the quality and quantity of data gathered according to the different purposes of the network monitoring and 'anonymization' of data

- Back end: solutions to manage access procedures (who can access what data), data processing operations and to control reversing of data in a clear format when necessary

Preliminary regulatory assessement

- March 2009 (Deliverable 2.3.1)
- EuroPriSe Criteria (European Privacy Seal, v. 0.3)
- Privacy matrix: law provision, technical solution and assessement
- Assessement against EU Directives 95/46/EC (Data Protection Directive); 2002/58/EC (e-Privacy Directive) and 2006/24/EC (Data Retention Directive)

Preliminary regulatory assessement 2

- PRISM appears to be privacy compliant at this stage
- Further fine-tuning is necessary to adapt the system to the specific national privacy law provisions: need of high flexibility
- Some provisions are not applicable since out of the scope of the PRISM project (e.g. data subjects' rights) and have to be fulfilled by the entity implementing the PRISM solution

Legal implications of network monitoring: privacy threats and requirements

Questions???

Francesca Gaudino
Baker & McKenzie Milan – Italy
francesca.gaudino@bakernet.com