Data protection
ensuring privacy

Ewan Sutherland

Contents

- Introduction
- OECD
- European Union
- Conclusions
- Issues

Trans-border data flows

- Increasing pressure to collect and share personal data within and across borders
- Increasingly interconnected systems and networks
- Growth of international trade:
  - e-commerce
  - outsourcing
- Intensification of cooperation against terrorism and crime

OECD principles

- Collection Limitation Principle
  - There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
- Data Quality Principle
  - Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
- Purpose Specification Principle
  - The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
- Use Limitation Principle
  - Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:
    - a) with the consent of the data subject; or
    - b) by the authority of law.
- Security Safeguards Principle
  - Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

OECD principles (2)

- Openness Principle
  - There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
- Individual Participation Principle
  - An individual should have the right:
    - a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
    - b) to have communicated to him, data relating to him
      - within a reasonable time;
      - at a charge, if any, that is not excessive;
      - in a reasonable manner; and
      - in a form that is readily intelligible to him;
    - c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and
      d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.
- Accountability Principle
  - A data controller should be accountable for complying with measures which give effect to the principles stated above.

http://www.oecd.org/sti/security-privacy

Council of Europe

- Convention 108
- Transborder flows to a country Party to the Convention cannot be forbidden or submitted to authorisation
- Exceptions:
  - no equivalent protection in the third country of specific categories of data [or no adequate protection]
  - re-exportation could circumvent the protection

United Nations

- 1990 “Guidelines for the Regulation of Computerized Personal Data Files”
- Free circulation if *comparable safeguards* for the protection of privacy

http://www.unhchr.ch/html/menu3/b/71.htm

European Union

- Directive 95/46/EC
- Free circulation within EU, and beyond if adequate level of protection
- The European Commission can negotiate with third countries
- Exceptions:
  - consent
  - contract
  - justice
  - public interest
  - vital interest of the data subject
  - public registers
  - adequate safeguards

European Union (2)

- Directive 2002/58
- part of the EU regulatory framework for electronic communications:
  - technology neutrality
  - updated definitions
  - opt-in for unsolicited e-mails
  - clarification on use of cookies
  - admissible use of traffic data
  - new rules on location data
  - opt-in for subscriber directories
  - clarification on data retention
- Traffic Data Retention Directive

Data protection authorities

- Independent national authorities
- Consulted by government in drawing up administrative measures or regulations
- Hear claims lodged by data subjects
- Inform data subjects and data controllers of their rights and duties
- Receive notifications, issue prior opinions and authorizations of certain processing operations
- Play an “alert function” on privacy risks incurred by new developments
- Work together in the EU through Article 29 Working Group
- Also participate in the work of the OECD

United Kingdom

- Data Protection Act 1998
- Enshrines eight data protection principles in UK law
- Personal information of a living individual must be:
  1. processed fairly and lawfully
  2. processed only for specified purpose(s)
  3. adequate, relevant and not excessive
  4. accurate and kept up to date
  5. kept no longer than necessary
  6. available to data subjects
  7. processed in such a way to prevent breaches of the principles
  8. transferred only to 'white-list' countries

http://www.dataprotection.gov.uk/

Asia-Pacific Economic Cooperation

- 2004 Privacy Framework
- Exporter to ensure *protection of the information in accordance with the principles*.
- Otherwise, other means should maintain *consistency* with the principles (e.g. obtaining consent)

Non-legislative approaches

- Self-regulation:
  - best practices
  - binding corporate rules
  - audit and certification
  - trustmarks and seals
- Independent oversight
- Model contract clauses
- Technological solutions
  (e.g. Privacy Enhancing Technologies (PETs))

Airline reservations to the USA

- Government of the USA asked foreign airlines to disclose data on all passengers flying there
- Wide range of data
- Purposes were not disclosed
- Period of retention was not disclosed
- Seen to breach EU data legislation

RFID

- Concern at this new technology
- Will it be secure?
- Will it be safe?
- Will tags be erased?
- How easily can they be read?

Questions for senior management

- Does the company operate in any part of the world where it is required to comply with privacy and data protection laws and regulations?
- Does the company have in place privacy and data protection risk management processes?
- Could the company be subject to fines and penalties for failing to comply with applicable laws and regulations?
- If a privacy debacle were to occur, could the resulting loss of customer trust irreparably damage the company's reputation?
- Does the success of the company's business model or the growth of its customer base depend on establishing trust with users regarding the protection of personal identifying information?
- What does the company stand to gain or lose by addressing or not addressing the privacy concerns of customers?
- Does the company have a comprehensive, clearly articulated public privacy notice?
- What steps does the company take to ensure that all employees of aware of the privacy program requirements?
- Does the company treat personally identifiable information with the same high standard of care whether it is collected off-line to on-line?
- Has the company developed a comprehensive Privacy Program, headed by a Privacy Officer and allocated the appropriate resources?

Conclusions

- Broad agreement on OECD principles
- Differences in implementation
- Increasing potential for data to be transferred
- Increasing risk of data exposure
- Compliance is a legal obligation and commercial necessity

Ewan Sutherland

- http://.www.3wan.net/
- 3wan [at] 3wan.net
- ewan [at] gstit.edu.et
- skype://sutherla