The OECD Trust Agenda: Promoting Security and Confidence

Sarah Andrews
16 May, 2006

- **Purpose**
  - **fulfil promise for economic and social development**
- **Scope**
  - **the system / network**
  - **the user**

The System / Network

- Viruses
- Denial of service
- Web page hijacking
- Spam

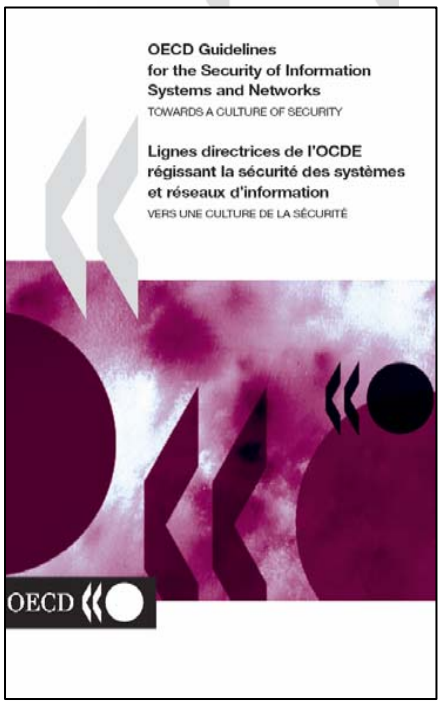
The User

- Unauthorised collection or use of personal information
- Identity theft
- Fraud
- Breach of consumer protection rules or expectations
- Spam

Policy response

- Promoting a **culture of security**
- Protecting **individual privacy**
- Ensuring **consumer protection**
- Tackling **spam**

Guidelines for the Security of Information Systems and Networks (2002)



***Objective**: Guide a coordinated implementation of policies and practices and create a cultural change in the way society perceives information technology security*

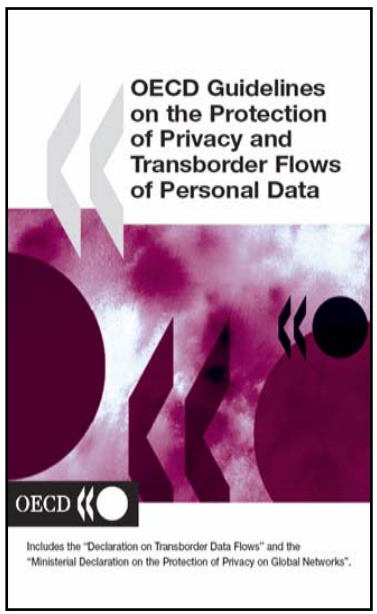
- Aimed at all "participants" (governments, businesses, civil society, end users)
- 9 high-level policy and operational principles
  - need for security
  - steps to enhance security

Principles of the Security Guidelines

Principle	Description
Awareness	Participants should be aware of the need for security of ISN and what they can do to enhance security
Responsibility	All participants are responsible for the security of ISN
Response	Participants should act in a timely and cooperative manner to prevent, detect and respond to security incidents
Ethics	Participants should respect the legitimate interests of others
Democracy	The security of ISN should be compatible with essential values of a democratic society
Risk Assessment	Participants should conduct risk assessments
Security Design and Implementation	Participants should incorporate security as an essential element of ISN
Security Management	Participants should adopt a comprehensive approach to security management
Reassessment	Participants should review and reassess the security of ISN and make appropriate modifications to security policies, practices, measures and procedures

Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980/1998)

Objective: *help to harmonise national legislation in order to uphold individual privacy rights while at the same time preventing interruptions in flows of data.*

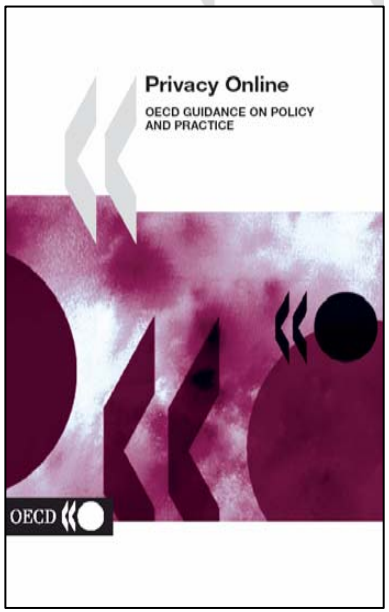


- 8 principles for the collection and management of personal data
- flexibility of application: all media; all types of processing; all categories of data
- 1998: re-affirmed commitment to ensure privacy on global networks

Principles of the Privacy Guidelines

Principle	Description
Collection limitation	There should be limits to the collection of personal data and all such data should be obtained by lawful and fair means
Data quality	Personal data should be relevant to the purposes for which they are to be used and should be accurate, complete and up to date.
Purpose specification	Purpose for which personal data are collected should be specified upfront and should not be used for incompatible purposes
Use limitation	Personal data should not be disclosed or used for purposes other than those specified without consent or authority of law
Security safeguards	Reasonable safeguards should be put in place to guard against risks such as loss, unauthorised access; destruction; modification of personal data
Openness principle	There should be a general policy of openness about the handling of personal data and means made available to establish the existence and nature of personal data.
Individual participation	Individuals should be able to ascertain whether data is being maintained on him/her and be given the opportunity to challenge any errors in that data
Accountability	Should be laws in place to ensure that data controllers are accountable for complying with these principles.

Privacy Online – OECD Guidance on Policy and Practice (2002)



"OECD member countries, business, other organisations, individual users should all give effect to the OECD recommendations and take further steps to help ensure privacy protection online at both national and global levels."

Recommendations at the national level

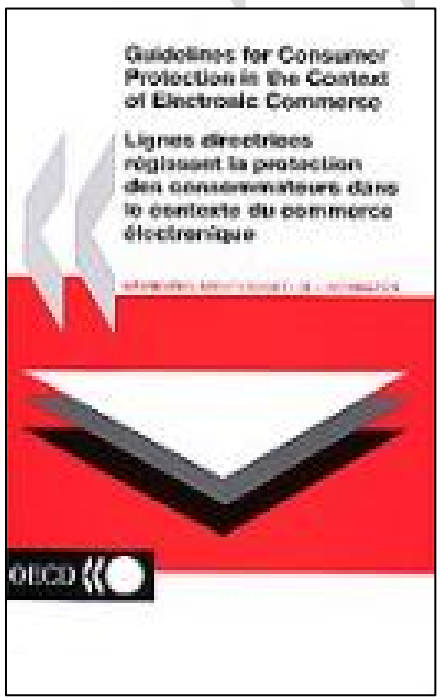
- Adoption of privacy policies
- Online notification of privacy policies to users
- Availability of enforcement and redress mechanisms in cases of non-compliance with privacy principles and policies
- Promotion of user education and awareness about online privacy and the means of protecting privacy
- Use of privacy-enhancing technologies and development of privacy functions in other technologies

Recommendations at the global level

- Improvement of bi- and multi-lateral mechanisms for X-border co-operation between public enforcement agencies.
- Co-ordination with the private sector and exploration of public/private partnerships in areas where technology and regulation are closely interrelated.
- Promotion of co-operation with other international organisations.
- Exploration of ways to further online trust across all participants through outreach, education, co-operation and consultation.

Consumer Protection Guidelines (1999)

***Objective**: Ensure that consumers no less protected when shopping online than when buying from their local store or ordering from a catalogue*



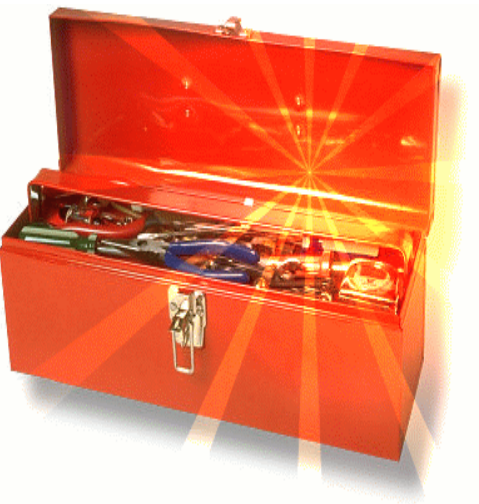
- Fair business, advertising and marketing practices
- Online Disclosures
- Transparent confirmation process
- Secure payment mechanisms
- Dispute Resolution and Redress
- Privacy protection
- Global co-operation against bad actors

Guidelines for Protecting Consumers from Cross-Border Fraud (2003)

- Domestic frameworks
  - Effective frameworks of laws and institutions to limit and take enforcement action against fraud
  - Effective investigative tools
  - Effective measures for individuals to obtain redress
- Principles for international co-operation
  - Use of international networks and arrangements
  - Notification, information sharing, investigative assistance, and confidentiality
  - Jurisdiction to protect foreign consumers
- Private sector co-operation
  - education and awareness
  - Referral of complaints
  - Investigative assistance

The Anti-Spam Toolkit: recommended policies and measures

- Regulatory approaches
- Enforcement
  - Recommendation on Cross-Border Spam Enforcement Co-operation
- Industry driven initiatives
- Technical solutions
- Education and awareness tools
- Co-operative partnerships against spam
- Spam metrics
- Global co-operation (Outreach)



Commonalities

- Strong prevention:
  - risk assessments
  - information sharing
  - technical safeguards
  - education and awareness raising
- Rapid and effective response:
  - law enforcement tools
  - industry / technical initiatives
  - individual redress mechanisms
- Ongoing co-operation:
  - International co-operation
  - Public/private partnerships

Measuring Trust

- Scoping Study on the Measurement of Trust in the Online Environment
  - Part 1: reviews official data from NSOs
  - Part 2: reviews semi-official data (Government but not NSOs such as Consumer Policy, Law Enforcement)
  - Part 3: reviews private sources of data (all other sources including security firms and industry groups, Internet bodies such as CERTs, consulting companies etc) as well as industry statistics on selected phenomena (phishing, spyware, viruses)

Model surveys: questions on trust (security and privacy)

- Business
  - Web presence (security policy statement, Security seal or certification, Privacy Policy Statement, Privacy seal or certification).
  - Security Measures (Virus checking, Anti-spyware, Firewall, Secured communication, Intrusion detection, IT security training, Data back-up (offsite), None
  - Problems Encountered (Virus, Trojans, Worm, Denial of Service, None) Limitations to buying/Selling on Internet (Security, Privacy)
- Household/Individual
  - Reason for not having access (Skills, Harmful content, Privacy, Security)
  - Problems encountered and damage caused (Virus, Trojan, Worm)
  - Software protection (Anti-Virus, Firewall, Anti-Spyware)
  - Reasons for not buying or ordering goods or services over the Internet (Trust Security, Privacy)

Measuring Trust: ongoing

- Use this work as basis for publication of indicators (e.g. in Science Technology Industry Scoreboard)
- Encourage the development of definitions, tools and concepts to assist in comparable measurement

In 2005 phishers used a fake US Census Bureau email/website scam!

More information

- **Security/privacy**

www.oecd.org/sti/security-privacy

www.oecd.org/sti/cultureofsecurity

- **Consumer protection and cross-border fraud**

www.oecd.org/sti/consumer-policy

- **Anti-spam**

www.oecd-antispam.org

- **Measuring trust**

www.oecd.org/sti/measuring-infoeconomy