



www.coe.int/cybercrime

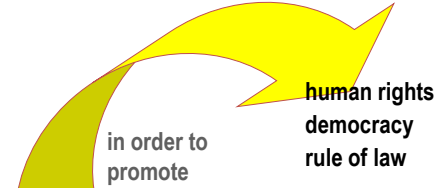
European Dialogue on Internet Governance

## Security and privacy: what are the issues?

Workshop 4: Cybercrime and -security  
Geneva, 14-15 September 2009

Alexander Seger  
Council of Europe,  
Strasbourg, France  
Tel +33-3-9021-4506  
alexander.seger@coe.int

About the Council of Europe ... www.coe.int



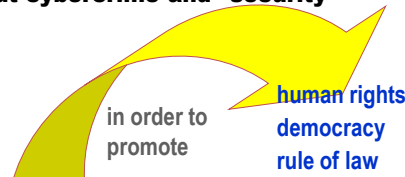
Measures against economic and organised crime



Established in 1949  
Currently 47  
member States

www.coe.int/cybercrime

About cybercrime and -security



Strategies against cybercrime

➤ Build human rights, democracy and the rule of law into anti-cybercrime and cybersecurity strategies

www.coe.int/cybercrime

About privacy and data protection

Why data protection and privacy?

- Article 8 ECHR: Everyone has the right to respect for his private and family life, his home and his correspondence.
- Data protection essential for the development and fulfillment of one's personality
- Condition for self-determination
- Protecting freedom of expression
- Protecting human dignity
- Preventing control and manipulation
- Precondition for freedom and democracy
- Prevention of crime

www.coe.int/cybercrime



Vision of a totalitarian State where "big brother is watching you" at any time, where the aim of the party is to "extinguish once and for all the possibility of independent thought".

One of the problems that the party needs to resolve is "how to discover against his will what another human being is thinking".

This is the role of the Thought Police:  
"A Party member lives from birth to death under the eye of the Thought Police. Even when he is alone he can never be sure that he is alone. Wherever he may be, asleep or awake, working or resting, in his bath or in bed, he can be inspected without warning and without knowing that he is being inspected. Nothing that he does is indifferent. His friendships, his relaxations, his behaviour towards his wife and children, the expression of his face when he is alone, the words he mutters in sleep, even the characteristic movements of his body, are all jealously scrutinized. Not only any actual misdemeanour, but any eccentricity, however small, any change of habits, any nervous mannerism that could possibly be the symptom of an inner struggle, is certain to be detected. He has no freedom of choice in any direction whatever."

About privacy and data protection

Data protection standards:

- OECD 1980: Guidelines on the Protection of Privacy and Transborder Flows of Personal Data
- Council of Europe 1981: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108) [Opened for signature on 28 January 1981 -> data protection day] + Protocol on supervisory authorities (ETS 181 of 2001)
- Council of Europe 1987: Recommendation R (87) 15 regulating the use personal data in the police sector
- EC Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data
- Positive obligation of governments to ensure data protection
- Latest proposals by CoE Data Protection Committee (T-PD):
  - Proposal for a CoE recommendation on profiling
  - Proposal to update Convention 108

www.coe.int/cybercrime

**Principles of data protection**

Personal data are defined as "any information relating to an identified or identifiable natural person ("data subject")"

EU Article 29 Working Party (2008):  
IP addresses are personal data in particular when correlated with unique ID cookies

- "fair collection principle" (personal data should be gathered by fair and lawful means)
- "minimality principle" (the amount of personal data gathered should be limited to what is necessary to achieve the purpose(s) of gathering the data)
- "purpose specification principle" (personal data should be gathered for specified and lawful purposes and not processed in ways that are incompatible with those purposes)
- "use limitation principle" (use of personal data for purposes other than those specified should occur only with the consent of the data subject or with legal authority)
- "data quality principle" (personal data should be accurate, complete and relevant in relation to the purposes for which they are processed)
- "security principle" (security measures should be implemented to protect personal data from unintended or unauthorised disclosure, destruction or modification)
- "individual participation principle" (data subjects should be informed of, and given access to, data on them held by others, and be able to rectify these data if inaccurate or misleading)
- "accountability principle" (parties responsible for processing data on other persons should be accountable for complying with the above principles)

**About privacy and data protection**

Privacy is more than the right to be left alone.

It is about

- self-determination and human dignity
- the right of a person to determine him-/herself the development and fulfillment of his or her personality
- the freedom to act in a given context
- exercising fundamental rights such as the freedom of expression, of assembly, thought, conscience, religion etc
- the functioning of a democratic society
- the power of a person to decide what information about him or her is disclosed and within which limits

**Data protection/privacy challenges**

- Our data increasingly stored on computer systems
- Transborder flows of data / data stored in different countries: what protection of data stored elsewhere?
- Linking of data (less distributed)
- Data protection concerns related to trends in technology: Data stored in the clouds, interoperability of devices, IPv6, DNSSEC, etc.

**Data protection/privacy challenges**

Our data are wanted by many. For example:

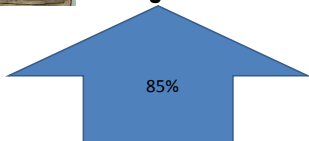
- Private sector
  - Financial services (SWIFT, Schufa, Online banking, credit card companies)
  - Search engines and related webservices (IP addresses, unique computer ID cookies, search/use protocols, scans of email contents etc.)
  - Social networks
  - Data and marketing services (compiling data on individuals)
- Governments
  - Security, law enforcement, prevention/control of terrorism etc
  - Data retention
  - Access to private sector data
- Criminals
  - Phishing and other types of fraud and cybercrime



Superego



Ego



Unconscious = It = Information technologies?

**About cybercrime and -security**

- Public and private infrastructure depend on ICT
- Society relies on ICT to the extent that the confidentiality, integrity and availability of computer data is a basic right
- Security of ICT at risk through cybercrime
- Key problem: Anonymity / lack of traceability
  - "cybercriminals are successful because people, machines, software and data are not well authenticated" (Scott Charney)
  - "anonymity is the key issue (Eugene Kaspersky).
- Problem enhanced through privacy enhancing technologies, encryption etc?

**International standards against cybercrime**

“Budapest” Convention on Cybercrime

A global framework for

- Making conduct a criminal offence (substantive criminal law)
- Providing law enforcement with tools for efficient investigations (procedural law)
- Allowing for efficient international cooperation

Compatible with data protection standards  
Can help promote data protection standards

**Standards against cybercrime**

**Guidelines for the cooperation between law enforcement and internet service providers against cybercrime**

Adopted at the global Conference on Cooperation against Cybercrime (Council of Europe, Strasbourg, 1-2 April 2008):

- Common measures (including protection of rights and freedoms)
  - Measures to be taken by law enforcement
  - Measures to be taken by service providers
- = LEA and ISPs need to cooperate but base this cooperation on law and clear, formalised procedures
- = They should cooperate for the protection of rights and freedom of individuals

**Enhance security through authentication**

**Need**

- strong authentication of hardware, software, people, and data; and
- improving the ability to audit events to provide accountability
  - Identity claims re person, device or software
  - Authentication to verify ID claim
  - Authorization policies
  - Access control mechanisms
  - Audit

Scott Charney 2008: Establishing End to End Trust. (Microsoft)

**Need**

- internet passports for individuals
- accreditation for businesses

Eugene Kaspersky at CoE Octopus Conference March 2009

**Implications/risks**

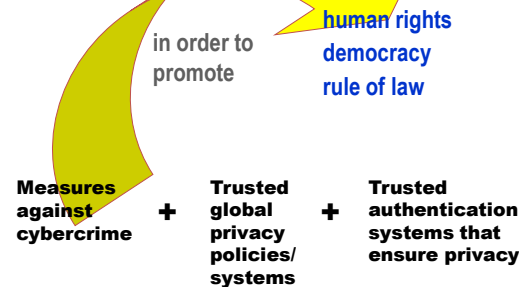
- Personal data as targets
  - + Interoperability of devices
  - + Transborder data flows
  - + Cloud computing
  - + Variations in data protection/privacy standards
  - + Fight against crime
  - + IPv6/new technologies
- + authentication**



= Conditions for linking up all (previously separated) data on individual persons?

**Conclusion**

Security and privacy – the core challenges



Thank you.

Alexander.seger@coe.int