Legal Aspects of the MonIKA-Project - Privacy meets Cybersecurity

Sebastian Meissner

Security Incident Information Sharing Workshop

Berlin, 26.07.2013

SPONSORED BY THE
Federal Ministry of Education and Research

MonIKA

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Introduction

- Opening question

  Privacy & cybersecurity: a mismatch?

- Alternative opening question

  Privacy & cybersecurity: two sides of the same coin?

- The notion of privacy

  In this presentation, the term privacy comprises two main aspects:

  - Data protection ("data privacy")
  - Confidentiality of communications

Data protection

- Art. 8(1) of the EU's charter of fundamental rights

  "Everyone has the right to the protection of personal data concerning him or her."

  → Data protection is a fundamental right

- Basic principles
  - Controller / processor
  - Legal basis (e.g., consent, contract)
  - Principle of necessity
  - Transparency (information duties, right of access)
  - Principle of purpose specification and limitation
  - Technical and organisational measures ("data security")

Confidentiality of communications

- Art. 7 of the EU's charter of fundamental rights

  "Everyone hast the right to respect for his or her [...] communications."

- Art. 5(1) of Directive 2002/58/EC ("ePrivacy Directive")

  "Member States shall ensure the *confidentiality of communications* and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation."

  Exceptions:

  - Consent of the users concerned
  - Legal authorisation (e.g., for law enforcement agencies)

Two sides of the same coin

- Data security

  Security of personal data is one crucial aspect of data protection

- Legal requirements

  "Controller must implement appropriate technical and organizational measures to protect personal data against [...] unlawful forms of processing."

  E.g., physical and logical access control, encryption, backup & recovery

- Cybersecurity

  A high level of cybersecurity contributes to the overall level of data security → data protection benefits from a high level of cybersecurity

Privacy and cybersecurity: a mismatch?

- Problem description

  Measures to ensure a high level of cybersecurity may

  - entail the processing of personal data
  - interfere with the confidentiality of communications

- Typical measures

  Examples for typical measures (MonIKA use cases) are

  - Detection and analysis of spam emails → identification of botnets
  - Monitoring of internet routing
  - Exchange of relevant data between different organisations (e.g., for the purpose of detecting anomalies / potential threats)

Privacy and cybersecurity: a mismatch? (II)

- Processed data

  Examples for types of personal data that may be processed in the "cybersecurity context" are

  - IP addresses (European Court of Justice in SABAM ruling (2011): "IP addresses, which are personal data")
  - email addresses
  - contents of emails (potentially including "sensitive data")
  - contact data of employees that are competent for cybersecurity

- Compliance with basic principles

  Legal obligation to comply with the basic principles listed on slide 3

Privacy and cybersecurity: a mismatch? (III)

- Approaches to a solution
  - Informed consent of all data subjects concerned
  - Data avoidance & minimisation, in particular anonymisation and pseudonymisation

    Examples:
    - Aggregation of data
    - Truncation of IP addresses
    - Replacement of an email by a description of that email (summary of specific characteristics) → currently examined within MonIKA

- "Draft answer"
  - Privacy by design may enable both strong data protection and efficient measures contributing to a high level of cybersecurity
  - Possibility to provide legal certainty by means of specific legislation

EU Legislation

- EU Commission's proposal for a network and information security (NIS) Directive
  - Member States must adopt a NIS strategy and designate a national NIS competent authority
  - Creating a cooperation mechanism among Member States and the EU Commission to share early warnings on risks and incidents
  - Operators of critical infrastructures, enablers of information society services and public administrations must adopt risk management practices and report major security incidents

  Art. 1(5): General reference to Data Protection Directive 95/46/EC

  No specific, comprehensive rules on data protection in the proposal

EU Legislation (II)

- Directive on attacks against information systems
  - Status: Adopted by EU Parliament on 4 July; yet to be approved by EU Council
  - Content: New rules concerning the definition of criminal offences and the sanctions in the area of cybercrime

    Inter alia:
    - Maximum penalty of at least three years when a significant number of information systems have been affected through the use of a tool → e.g., *botnets*
    - Maximum penalty of at least five years when the offense causes serious damage or when the offense is committed *against a critical infrastructure information system*