Privacy in IETF Protocols

Professor Ian Walden
Centre for Commercial Law Studies, Queen Mary, University of London
Of Counsel, Baker & McKenzie

BAKER & MCKENZIE

Introductory Remarks

- Privacy & data protection laws
  - Legal obligations
    - data processing principles
  - Supervision & enforcement
- Case studies
  - Cookies
  - Call-ID
- PETs & privacy by design
- Considerations for developers

Privacy laws

- European Convention on Human Rights, Art. 8
  - (1) Everyone has the right to respect for his private and family life, his home and his correspondence.
  - (2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.
- Privacy remedies
  - Constitutional, tortious, equitable, contractual, copyright, defamation, computer misuse.....

Data Protection Laws

- European Union
  - Charter of Fundamental Rights, Art. 8
  - Directives 95/46/EC (general) & 02/58/EC (privacy and electronic communications)
    - Reform proposals (25 January 2012)
- Characteristics
  - Personal data
  - Justified basis for processing
  - Right of access
  - Independent authority

Personal data

- ‘an individual can be identified directly or indirectly’
  - “all the means likely reasonably to be used” (recital 26)
  - Anonymity & pseudonymous techniques
- Case study: IP addresses
  - Generating & maintaining logs
- ‘special categories of data’: sensitivity
  - racial/ethnic origin, political, religious or philosophical beliefs, trade-union membership, health or sex life, criminal data
  - ‘traffic data’ & ‘location data’

Processing principles

- Collection
- Proportionality
- Use
- Data Quality
- Transparency
- Access and Correction
- Objection
- Transfers
- Security
- Accountability

Collection

- Data to be fairly and lawfully obtained
- Consensual processing
  - Data subject consent: ‘freely given, specific, informed’
  - Explicit or implicit: ‘opt-in’ or ‘opt-out’
- Non-consensual processing
  - Necessary for specified (and limited) reasons
    - e.g. EU Directive 06/24/EC on data retention
- Ability to exclude data from certain processing

Proportionality

- Personal data should be adequate, relevant and not excessive to the purpose for which it is collected

Use Limitation

- No disclosure, transfer or other use except those needed to achieve the purposes specified except:
  - With consent of data subject
  - Pursuant to law
    - e.g. employer tax reporting

Data Quality

- As needed for specified purposes, collected and stored data should be accurate, complete & up-to-date

Transparency

- Data subjects should have the means to know existence and nature of processing; purposes of their use; the identity and location of the entity controlling the processing; whether any data is likely to be transferred and to whom

Security

- Appropriate measures by data controller to guard against:
  - Loss or destruction of data
  - Unauthorised processing or disclosure
- “Appropriate” to risk presented
  - Nature of data & processing
- Technological, organisational measures
  - “at the time of the design of the processing system and at the time of the processing itself” (recital 46)
  - Standards, e.g. IS0 27001
  - Security breach notification

Case study: Cookies

- IETF ‘HTTP State Management Mechanism’
  - rfc 2109 (1997); rfc 2965 (2000) & rfc 6265 (2011)
    - Session, persistent, 3rd parties
    - Default implementation: non-disclosure
- Directive 02/58/EC, art. 5(3)
  - Storing or accessing stored information on the user’s terminal equipment
    - Cookies, spyware, web bugs.....
  - From notification to consent

Case study: Call-ID

- Directive 02/58/EC, art. 8
  - Calling and connected line identification: per call or line
  - Balancing privacy interests of communicating parties
  - Override for Law enforcement requirements & emergency services
- IETF INSIPID: ‘end-to-end session identifier’
  - REQ5: The identifier must not reveal any information related to any SIP device or domain identity, including IP Address, port, hostname, domain name, username, Address-of-Record, MAC address, IP address family, transport type, etc.
    - i.e. Call-ID header field without host information – ‘topology hiding’
  - REQ8: The identifier should be unique in time and space, similar to the Call-ID

Privacy Technologies

- Privacy- Enhancing Technologies (PETs)
  - Privacy Management Systems (PMS) & Identity Management systems (IMS)....
- Standards-making
  - CEN/ISSS ‘Initiative on Privacy Standardization in Europe’ (2002)
- Processing principles: Proportionality & security
  - Data minimisation
  - Reform proposal, art. 23: ‘data protection by design and default’

Considerations for developers

- Recognising regulated subject matter: ‘personal data’
- Always consider data minimisation
- Deploy anonymisation techniques
- More guidance in rfcs