Retention of traffic data in Norwegian legal context

Dr. Lee A. Bygrave
Assoc. Professor, Dept. of Private Law, University of Oslo
<lee.bygrave@jus.uio.no>
<http://folk.uio.no/lee>

Presentation, University of Bergen
14 May 2008

Current Norwegian rules

- Retention governed by Electronic Communications Act § 2-7 and license (konsesjon) issued by Data Inspectorate (Datatilsynet)
- Principal rule = data registered for billing purposes shall be deleted when billing done or deadline for complaint has passed
  - Quarterly billing: deletion at latest 5 mths after registration
  - Monthly billing: deletion at latest 3 mths after registration
  - If billing dispute, deletion once dispute settled

Police access to traffic data (1)

- Pt. of departure: telcos must maintain confidentiality of communications (E-Comm. Act § 2-9), but duty qualified to permit police access
- Police can req. disclosure of t.d. if reasonable ground (*skjellig grunn*) for suspecting criminal conduct resulting in 5 or more yrs of imprisonment; disclosure must be of essential significance (*vesentlig betydning*) for investigation: Criminal Procedure Act (CPA) §§216b-216c.

Police access to traffic data (2)

- Prior judicial approval usually req´d., cf. CPA §216d
- Police cannot go on general fishing expeditions
  - See interlocutory judgment of Supreme Court, Rt. 1999, p. 1944

Past Norwegian debate about t.d.

- SenTaks system in early 1990s
  - Registration of t.d. for specified billing
  - Paradigm shift
  - Data Inspectorate's initial decision (Feb. 1993) overturned by Ministry of Justice on appeal from Televerket (now Telenor)
- Little significant public debate since, despite…
  - EU Draft Framework Decision on data retention (2002)
    - » Proposed storage between 12 and 24 mths
  - Council of Europe Cybercrime Convention (2001)
    - » Art. 16(2): storage up to 90 days (renewable)

Data Retention Directive and Norwegian status quo (1)

- DRD introduces several new elements, such as …
  - Storage of geo-localisation data
  - Storage of email logs
  - Storage of Internet (dis-)connection times, IP-addresses used
  - More organisations affected by storage rules
  - Longer storage time (but unclear *how* much longer)
  - New normative basis for retention (*duty* to retain for purpose other than billing or communication)

Data Retention Directive and Norwegian status quo (2)

- Is “mass surveillance” (*overvåking*) apposite description of DRD’s impact?
  - Even if not, there exist significant and legitimate concerns -- e.g., poor security culture(s) of telcos, ISPs
- Yet policing concerns are also legitimate
  - Problem with flat-fee pricing
  - Possible “Free State” problem
    - » (Challenge for police to document their concerns)

Future impact/status of Directive (1)

- DRD difficult to interpret
  - E.g., provisions on Internet
- EU member states given considerable margin for manouvre
  - E.g., what = “serious crime”?
  - E.g., storage time (6 mths to 24 mths)?
  - E.g., what can be stored? (browsed URLs?)

Future impact/status of Directive (2)

- Is Directive ultra vires?
  - First pillar vs. Third pillar
  - Ireland v. Council and Commission, Case C-301/06
  - ECJ decision on PNR Agreement (judgment of 30 May 2006 in Joined Cases C-317/04 and C-318/04)
- Can Directive be lawfully appended to EEA Agreement?
- Norway's veto power -- worth exercising?