JUR 5630 – 2010
Lecture 9
EU legislation on privacy and e-communications
(18th March 2010)

Lee Bygrave

1. Disposition

- Normative background – ECHR Article 8; national legislation
- Directive 2002/58/EC
- Directive 2006/24/EC

2. Normative background

- ECHR Article 8(1) – "respect for private life … and *correspondence*".
- Fairly large number of ECtHR decisions on communications privacy: see, e.g., …
    1. *Klass v. Germany* (1978)
        - ECtHR holds for first time that telephone conversations are covered by notions of "private life" and "correspondence" (see para. 41).
    2. *Malone v. UK* (1984)
        - Focused on lawfulness of use of "metering" records.
    3. *Kruslin v. France* (1990)
        - Focused on lawfulness of telephone tapping by police.
    4. *Copland v. UK* (2007)
        - Focused on lawfulness of employers' access to employees' email communications
- Protection of communications privacy also provided for in many national constitutions and/or other legislation: see, e.g., …
    1. Spain's Constitution Art. 18(3)
    2. Germany's Basic Law Art. 10
    3. Norway's Penal Code §§ 145, 145a
    4. Swiss Penal Code Art. 179.
- Case law of German Federal Constitutional Court particularly protective – see espec. 1 BvR 370/07, 1 BvR 595/07, 27.02.2008 (covert surveillance of ICT systems); 1 BvR 2378/98, 03.03.2004 (eavesdropping on private homes); 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, 02.03.2010 (retention of traffic data). Latter judgment dealt with further below.

3. Directive 2002/58/EC (ECD)

- Supplements and "fine-tunes" Directive 95/46/EC
    - Cannot be fully understood without consideration of latter (e.g., latter provides core definitions)
    - Has greater reach than DPD (e.g., in relation to protection of legal person data)
    - Still only example of sectoral EU data protection law (outside Third Pillar)
    - Some commentators query its necessity
- Replaces and repeals Directive 97/66/EC
    - Focus of latter too narrow (on traditional telephony plus ISDN)
    - Application to Internet was difficult to determine
- Basic purpose:
    1. provide for relatively detailed rules for protection of personal data that are processed in relation to certain e-communication networks and services;

2. harmonise national provisions on point;
3. create conditions for free movement of data.

- Part of broader regulatory package establishing Common E-Communications Framework, basic aim of which = increase competition in e-communications market; other aim = protect consumers and users of e-communications networks/services (*viz.*, course material in JUR5640)
- Amended November 2009 by Directive 2009/136/EC (as part of amending e-communications regulatory framework generally): main amendments concern
    1. mandatory notification of personal data security breaches (Article 4(3));
    2. consent requirements for cookies (Article 5(3));
    3. anti-spamming measures by ISPs (Article 13(6)).
- Amendments to be implemented by June 2011.
- Consolidated version of Directive available at: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002L0058:20091219:EN:PDF.
- Scope of application set out in Art. 3: data processing in connection with provision of publicly available electronic communications services in public communications networks in the Community.
    - What = "electronic communication service"? See Framework Directive 2002/21/EC for electronic communications networks and services, Art. 2(c) (content and broadcasting not covered).
- Protection of certain "legitimate interests" of legal persons in role of subscribers/users of e-communications services, but this protection not fully commensurate with protection of individuals (see Arts. 12 and 13(1) dealing with respectively subscriber directories and automated calling systems)
- Central provisions deal with
    1. security and confidentiality of communications (Arts. 4–5)
    2. storage and use of communications traffic data (Arts. 6, 15)
    3. processing of location data other than traffic data (Art. 9)
    4. calling and connected line identification (Art. 8)
    5. content of subscriber directories (Art. 12)
    6. unsolicited communications for direct marketing purposes (Art. 13)
        - Basic rule: opt-in for spam
- Provisions dealing specifically with cookies, spyware and like
    - e.g., Art. 5(3) – requires organizations to obtain users' consent before placing cookies on their computers (previously cookies permitted only if receiver was informed and could refuse them)
    - how can consent be manifested? Does user consent when default Web browser setting is to accept cookies? Cf. recitals 17 and 25 in consolidated version of Directive 2002/58/EC; cf. recital 66 in Directive 2009/136/EC ("Where it is technically possible and effective, in accordance with the relevant provisions of Directive 95/46/EC, the user's consent to processing may be expressed by using the appropriate settings of a browser or other application").
- Encouragement of PETs
    - e.g., recital 9 and Article 14 (standardization of ICT so that it is privacy-friendly)
- Note CJ decision of 29.01.2008 in case C-275/06 *Promusicae v Telefonica de Música de España* (Held: Directive 2002/58/EC does not require ISPs "to communicate personal data in order to ensure effective protection of copyright in the context of civil proceedings", but Mbr States may introduce laws with such requirement, if not in conflict with fundamental rights or proportionality principle)

- Part of broad battle between IPR-holders and ISPs over access to IP address data and identities behind these.

4. Directive 2006/24/EC

- Response to terrorist attacks in Madrid (2004) and London (2005)
- Modifies effect of ECD with respect to traffic data
    - Basic rule in ECD is that traffic data must be erased except if needed for billing purposes (Art. 6)
    - Possibility for derogation in ECD Art. 15
- Basic requirement = member states to ensure that providers of public communications networks store traffic data (including location data) for minimum of 6 months and maximum of 2 years.
- Further temporary extensions permitted in case of specific threats.
- Does not cover data "revealing the content of … communication" (Article 5(2); see too Article 1(2) ("including information consulted using an electronic communications network"). Is there, in reality, a watertight distinction between traffic data and content data?
- Data retention for purpose of countering "serious crime" (Art. 1(1); recital 21). What = "serious crime"?
- Access to be given to "competent national authorities" (Art. 4). Latter not defined.
- Transposition by Sept. 2007 but delay possible until 15 March 2009 for Internet-related data (Art. 15(3)).
- Ireland (later joined by Slovakia) brought action claiming Directive is without proper legal basis in EU law (claimed that Directive = First Pillar instrument dealing with Third Pillar matters) (see Case C-301/06); ECJ held 10.02.2009 that Directive has proper legal basis.
    - Cf. ECJ judgment of 30.5.2006 in Joined Cases C-317/04 and C-318/04 regarding transfer of PNR data to USA (nullifying 2004 decisions by Commission and Council on PNR transfers because they applied to matters currently falling outside scope of Community law – namely, public security and prevention of crime).
- Many experts claim – with considerable persuasive power – that Directive violates ECHR Art. 8 (particularly proportionality principle).
- Many EU Member States had postponed until 2009 application of Art. 5 with respect to Internet-related communication, due to ambiguity of provision. Norway has still not transposed Directive.
- Decision of German Federal Constitutional Court: 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, 02.03.2010 (storage of traffic data is serious encroachment on interest protected by Constitution Article 10(1) but falls short of breaching that provision if there is "sufficiently sophisticated legislation with well-defined provisions on data security, in order to restrict the use of data, and for transparency and legal protection" – see further summary of judgment (in English) at: <http://www.datatilsynet.no/upload/Dokumenter/dommer/pressrelease_dataretention_bundesverfassungsgericht.pdf>. Court majority found that existing legislation did not meet requisite standards).
- See too decision of Romanian Constitutional Court 08.10.2009 (summarised in, i.a., <http://www.edri.org/edrigram/number7.23/romania-decision-data-retention>).
- Is Directive introducing a new paradigm regarding legitimation of surveillance techniques?