JUS5630 – 2013
Lecture 3
Overview of data protection laws, their aims and scope; laws o/side Europe
(14th February)

Lee Bygrave

1. Disposition

- Overview of data protection instruments
- Aims of data protection laws
- Field of application of data protection laws
- Laws outside Europe

2. Overview of international instruments

- Council of Europe Convention of 1981
- OECD Guidelines of 1980
  - NB. Guidelines on information security (1992 and 2002); guidelines on cryptography policy (1997); guidelines on consumer protection in context of e-commerce (1999)
- UN Guidelines of 1990
- EU instruments:
  - Directives 95/46/EC, 97/66/EC, 2002/58/EC, 2006/24/EC
  - EU Charter of Fundamental Rights (CFR), Article 8 (cf. Article 7) + Treaty on Functioning of the European Union (TFEU) Article 16: recognition in EU of data protection as fundamental right in itself; see too Treaty on European Union (TEU) Article 6(1) which gives CFR the "same legal value" as EU's Treaties
  - Council Framework Decision 2008/977/JHA regarding police and judicial cooperation in criminal matters
  - NB. Entire EU data protection framework is currently being revised!
- APEC Privacy Framework of 2004/05

3. Overview of national instruments (non-exhaustive)

- Hessen's Data Protection Act (1970)
- Sweden's Data Act (1973)
  - see now Personal Data Act of 1998
- USA's Privacy Act (1974)
- France's Law on Data Processing, Files and Individual Liberties (1977)
- Germany's Federal Data Protection Act (1977)
  - see now Federal Data Protection Act of 1990, as amended in May 2001
- Norway's Personal Data Registers Act (1978)
  - see now Personal Data Act of 2000
- Austria's Data Protection Act (1978)
  - see now Data Protection Act of 2000
- Canada's Privacy Act (1982)
  - see also now Personal Information Protection and Electronic Documents Act of 2000
- UK's Data Protection Act (1984)
  - see now Data Protection Act of 1998
- Australia's Privacy Act (1988)
  - see now too Privacy Amendment (Private Sector) Act of 2000
- Portugal's Data Protection Act (1991)

- see now Personal Data Protection Act of 1998

- Switzerland's Federal Data Protection Act (1992)
- New Zealand's Privacy Act (1993)
- Italy's Data Protection Act (1996)
- Poland's Data Protection Act (1997)
- Argentina's Data Protection Act (2000)
- Data Protection Acts passed in 2004 by Tunisia, Burkina Faso, Morocco and Mauritius
- Russia's Personal Data Act (2007)
- Dubai's Data Protection Act (2007)
- Bills in preparation in, a.o., South Africa, Malaysia, Thailand and Turkey

4. Aims of data protection laws

- Safeguard privacy, personal integrity etc.
- Ensure adequate information quality
- Ensure smooth TBDF (international instruments primarily)
- Promote realisation of Internal Market (DPD)
  - Cf. CJ decision in Joined Cases C-465/00, C-138/01, and C-139/01 *Österreichischer Rundfunk and Others* [2003] ECR I-4989 (emphasising human rights rationale of DPD)
- Ensure "informational equilibrium" between various State organs (some German laws only)
- Still considerable uncertainty over aims and rationale of data protection laws
  - Some laws lack objects clauses
- Note interest catalogues developed in Norwegian data protection discourse
  - Traditional catalogue: confidentiality; completeness; insight/participation; privacy; citizen-friendly administration; robustness; protection from abuse of power.
  - Cf. catalogue proposed by Bygrave 2002, chapter 7.

5. Ambit of data protection laws

5.1 Key concept = "personal data / information"

- What = "personal data/information"?
  - "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity": DPD Art. 2(a)
  - Basic criterion is identifiability
  - But many definitional issues:
    - What = identification?
    - How easily or practicably must a person be identified from the information?
    - Who is the legally relevant agent of identification?
    - To what extent must the link between a set of data and a person be objectively valid?
    - To what extent is the use of auxiliary information permitted in identification process?
    - What degree of individuation is required?
  - Recital 26 of DPD important in determining scope of "personal data" concept: "to determine whether a person is identifiable, account should be taken of *all* the means *likely reasonably* to be used *either* by the controller or by *any* other person to identify the said person"
  - Note attempts to cut back on prima facie scope of "personal data"
    - Court decisions

- *Durant v. Financial Services Authority* [2003] EWCA Civ 1746 (personal data must be "biographical in a significant sense"; it must go beyond simply registering a person's involvement "in a matter or event that has no personal connotations"; and it must have the individual "as its focus" – [28] per Auld LJ)
    - Cf. *R v. Rooney* [2006] EWCA Crim 1841 (defendant unable to avoid conviction for breach of DPA by running argument based on an interpretation of what = personal data similar to the interpretation given in *Durant*).
- *Eastweek Publisher Ltd & Anor v. Privacy Commissioner For Personal Data* [2000] HKCA 140
- *Harder v. The Proceedings* Commissioner [2000] NZCA 129
- Case T-194/04, *Bavarian Lager Co. Ltd. v Commission* [2007] ECR II-4523 (paras. 118–9): EU Court of First Instance (now "General Court") holds that not all personal data "necessarily fall within the concept of 'private life" or are "by their nature capable of undermining the private life of the person concerned"); decision has been appealed but outcome is as yet unknown

- What = "data"? Can biological material per se = data?
    - *S and Marper v UK* (2008): ECtHR says yes re CoE Convention (+ UK Data Protection Act).
    - For discussion and critique, see Bygrave, "The Body as Data? Biobank Regulation via the 'Backdoor" of Data Protection Law", *Law, Innovation and Technology*, 2010, vol. 2(1), pp. 1–25.

5.2 Trends

- Movement from regulating "registers" to "processing"
- From regulating only *computerised* processing/registers to manual processing also
- From regulating only *public sector* to private sector also
- Cf. USA and, to lesser extent, Japan and Australia
- From regulating information to regulating biobanks also (?)

5.3 Exemptions

- Police / national security
    - See, e.g., DPD Art. 3(2)
    - Cf. Council Framework Decision 2008/977/JHA regarding police and judicial cooperation in criminal matters
- Journalistic activity
    - See, e.g., DPD Art. 9
    - See CJ decision of 16.12.2008 in Case C-73/07, *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy, Satamedia Oy* [2008] ECR I-0000.
    - See Swedish Supreme Court decision in *Rambro* case (Case B293-00; 12.06.2001)
    - Cf. Norway's Personal Data Act 2000, § 7 ("opinion-formative" activity)
- Personal / domestic activity exemption
    - See, e.g., DPD Art. 3(2)
    - See ECJ decision in Case 101/01, *Bodil Lindqvist* [2003] ECR I-129711 (website publishing)

6. Laws outside Europe, with focus on Asia-Pacific

6.1 US law

- Large amount of case law on right to privacy
- Two main types:
    1. Constitution
    2. Tort
- Constitution: Landmark cases =
    1. *Griswold v. Connecticut*, 381 US 479 (1965) (accepting Constitutional right to "marital" privacy)
    2. *Katz v. United States*, 389 US 347 (1967) (holding that FBI placement of microphone in public telephone booth in order to bug telephone conversations breached Fourth Amendment)
    3. *Roe v. Wade*, 410 US 113 (1973) (accepting privacy claim for woman's decision whether or not to have abortion)
    4. *Whalen v. Roe*, 429 US 589 (1977) (holding that compulsory disclosure of patients' medical records does not necessarily constitute invasion of Constitutional right to privacy)
- There appear to be 3 types of "privacy" interests protected by Constitution:
    1. freedom from govt. surveillance and intrusion (4th Amendment)
        - Hinges on "reasonable expectation of privacy"
        - Controversial: see, e.g., *Smith v. Maryland*, 442 US 735 (1979) (deciding that "legitimate expectation of privacy" does not exist with regard to telephone numbers dialed from private home); *United States v. Knotts*, 460 US 276 (1983) (holding that "person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements").
        - "[T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence": *United States v. Miller*, 425 US 435 (1976) at 443.
    2. avoiding disclosure of personal matters (14th Amendment)
    3. independence in making important personal decisions (primarily 14th and 9th Amendments)
- What about interest in informational self-determination?
        - See, e.g., seminal analysis in P.M. Schwartz, "The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination", *American Journal of Comparative Law*, 1989, vol. 37, pp. 675–701.
        - Interest came up for review by Supreme Court in *NASA v. Nelson* 562 US _ (2011)(19.01.2011): Majority finds that Constitution protects informational privacy (Scalia and Thomas disagree) but that information sufficiently safeguarded under Privacy Acy 1974.
- Tort: 4 species identified
    1. intrusion into person's private affairs
    2. public disclosure of embarrassing facts
    3. publicity putting individual in false light
    4. misappropriation of person's name or likeness
        - See W.L. Prosser, "Privacy", *California Law Review*, 1960, vol. 48, p. 338–423.
- Legislation: no general data protection legislation; sectoral approach pertains. See, e.g., …
    1. Fair Credit Reporting Act (1970)

2. Privacy Act (1974)
3. Cable Communications Privacy Act (1984)
4. Video Privacy Protection Act (1988)
5. Electronic Communications Privacy Act (1986)
6. Children's Online Privacy Protection Act (1998)
7. Financial Services Modernization Act (1999) (Gramm-Leach-Bliley)

- Overall comparative assessment:
  Flaherty: "the United States carries out data protection differently than other countries, and on the whole does it less well" (D.H. Flaherty, *Protecting Privacy in Surveillance Societies* (Chapel Hill / London: University of North Carolina Press, 1989), p. 305). See also P.M. Schwartz & and J.R. Reidenberg, *Data Privacy Law: A Study of United States Data Protection* (Charlottesville: Michie Law Publishers, 1996), pp. 379–96.
    - A major concern = lack of federal privacy commission(er); piecemeal legislative regulation of private sector

6.2 Australia

- No recognition by major court of right to privacy at common law
- No right to privacy in Constitution
- Fairly extensive data privacy legislation at federal level
- Principal legislation = Privacy Act 1988
  Now covers both public and private sector but some large gaps re latter remain
    - employee records
    - small businesses
- Uneven regulation at state level
- Cp. Victoria and NSW with WA and SA.
- Cp. New Zealand's comprehensive Privacy Act 1993 – regarded as "probably the most effectively enforced law in the region" (Greenleaf), with relatively extensive body of case law. Main weakness in EU terms is lack of data export restriction.

6.3 Japan

- Act on the Protection of Personal Information held by Administrative Organs of 1988 – public sector coverage only;
- supplemented by Act on the Protection of Personal Information of 2003 covering private sector, albeit with exemptions for, i.a., mass media and small businesses (latter defined not in terms of annual turnover but numbers of data subjects in their databases).
- No central DPA.
- Act covering private sector does not create private right of action before judiciary; reliance instead on enforcement by relevant Ministries.

6.4 China

- Recognition of privacy-related interests in Constitution – Art. 38 (personal dignity); Art. 39 (illegal searches of or intrusion into private homes); Art. 40 (freedom and privacy of correspondence) – see <http://english.people.com.cn/constitution/constitution.html>.
- Protection of individual's reputation under Art. 101 of General Principles of the Civil Law of PRC: see <http://en.chinacourt.org/public/detail.php?id=2696>.
- International commitments? ICCPR signed but not ratified; APEC Privacy Framework has hitherto had little real purchase
- No general privacy/data protection legislation; some sectoral protections
    - E.g., Shanghai Municipal Interim Measures on Administration of the Collection of Personal Credits (regulating credit reporting)

- Proposal for Personal Information Protection Act, but final form and implementation unclear.
- PRC Tort Liability Law, adopted 26.12.2009 (in effect 01.07.2010): imposes liability in tort for infringement and damage of a wide ranger of "civil rights and interests", including privacy (隐私权); evidently establishes private rights of action in data subjects for mishandling of personal data
- PRC Criminal Liability Law – amended in 2009 to prohibit breaches of data security and illegal dissemination of personal data.
- "By not having a single conceptual underpinning to justify and shape a law that protects personal information, China today appears embarked on a path of establishing an uncoordinated patchwork of laws, each of which touches on personal information protection in its own distinct way, in its own context and with its own particular objectives. This could make management of personal information protection issues in China a complicated affair": Hunton & Williams Client Alert, January 2010.
- Cf. Hong Kong (SAR) – Personal Data (Privacy) Ordinance 1996
- Cf. Macau (SAR) Personal Data Protection Act 2006 (based closely on EU Directive)
- Cultural challenges in assimilating Western notion of privacy
    - Compare, e.g., newly introduced notions of "privacy" (隐私) and "privacy rights" (隐私权) as opposed to traditional Chinese notion of "hidden facts" (隐情), which pertains to criminal or immoral behaviour that is damaging to the public interest.

Further reading (in addition to pensum already listed):

James B. Rule & Graham Greenleaf (eds.), *Global Privacy Protection: The First Generation* (Cheltenham: Edward Elgar, 2008).