JUR 5630 – 2010
Lecture 13
Lex informatica and cyberspace (II)
(22nd April 2010)

Lee Bygrave

1. Disposition

- Code / l.i. and privacy interests
  - DRMS, P3P, PETs
  - Lessig's vision
- Code / l.i. and data protection law
  - Application of data protection law to cyberspace
  - Legislative support for PETs
  - Self-regulation vs. Co-regulation

2. Code and privacy interests

- Lessig: code is in the main hostile to privacy interests, but some forms of code (encryption; P3P) = best friend of privacy. Lessig recognises, though, that the latter code (P3P) is not enough to protect privacy; law is needed too – in Lessig's case, this law takes form of imposition of property right in personal data, together with contractual protections for exercise of that property right.
- Rotenberg: highly critical of Lessig – both in terms of characterisation of data privacy law and in terms of what = P3P.
- DRMS: potentially privacy-invasive (digital panopticon?); effect on browsers not just users of protected material

  - Unclear to what extent privacy law may ameliorate threats to privacy posed by DRMS
  - Copyright Directive (2001/29/EC) vs. data protection Directive(s)
    - May one circumvent monitoring devices without breaching Art. 6 of ©-Directive?
    - May one erase personal information about end-users without breaching Art. 7 of ©-Directive?
    - Note lack of symmetry between legislative protection for ©-tech and legislative protection for PETs
- What is basic message?

3. Application of data protection law to cyberspace

- Important question is NOT: do laws apply to Internet? But rather: HOW do they apply to Internet?
- Latter question leads to two further questions:
  1. Do the laws apply with sensible results?
  2. Do laws give sufficient prescriptive guidance?
- Most major data protection laws (e.g., Directive 95/46/EC (DPD)) drafted with little account of Internet
- Main exception = Directive 2002/58/EC (DPEC)
  - But note limitations on scope of application of DPEC
  - Key definitional issues left unresolved: e.g., scope of "personal data" concept with respect to e-mail addresses, IP addresses and attached clickstream data; status of electronic agents?
- Judiciary to rescue?
  - Little clarifying case law

    - BUT major ECJ decision in Lindqvist case – sensible decision?
- Risk of regulatory overreaching
    - Some instances in which application of data protection rules does NOT have entirely sensible results
    - Good example = DPD Art. 4(1)(c)

4. Legislative support for PETs

- Most data protection laws contain little direct support for PET use
    - DPD = case in point
    - Article 17 and recital 46 are concerned *prima facie* with security measures
- Difficulties in introducing more PET-specific rules, but these difficulties are surmountable
- Goals of anonymity (and/or pseudonymity) need to be specified more clearly, as do the means of their achievement (in terms of systems development)
- German legislation as possible model, cf. "Systemdatenschutz"

5. Role of netiquette

- Netiquette = useful but insufficient condition for ensuring respect for privacy in online environment
    - See, e.g., Computer Ethics Institute's "Ten Commandments for Computer Ethics"(<http://www.tekmom.com/tencommand/index.html>);
    - Virginia Shea's *Netiquette* (<http://www.albion.com/netiquette/>)
- Touted advantages: flexibility; user "ownership"; non-legalistic (hence simple) terminology
- Possible problems: "lightweight" normative effect; relatively transitory
    - Cf. Norway's "Net Tribunal" (Nettnemnda)

6. Co-regulation as preferred regulatory approach

- "Top-down" legislative action must be supplemented by "bottom-up" rule making
- Self-regulation by itself is insufficient; self-regulatory initiatives often more fruitful when threat that the state will otherwise "cover the field" through legislation
- Few co-regulatory schemes currently working with respect to Internet industry
    - Cf. Australia's Internet Industry Association Privacy Code of Practice (2001 draft) still awaiting approval
- Involvement of DPAs in Recommendations for Consideration (RFC) and other Internet standards?

7. Other strategies for privacy protection?

- "Mental hardwiring", starting in the schools …
- Some good examples –
    1. UK Information Commissioner's CD-ROM, "Protecting the Plumstones";
    2. EU's SAFT project (<http://ec.europa.eu/information_society/activities/sip/projects/completed/awareness/saft/index_en.htm>);
    3. Disney's "Surf Swell Island" (<http://disney.go.com/surfswell/>).
- But still much to be done on this front.
- Property approach?
- Note suggestions in Koops, B-J & Leenes, R., "'Code' and the Slow Erosion of Privacy", *Michigan Telecommunications and Technology Law Review*, 2005, vol. 12, issue 1, pp. 115–188.