

**JUS5630 – 2013**  
**Lecture 1**  
**Introduction to course**  
**(5 February 2013)**

*Lee Bygrave*

**1. Disposition**

- Overview of course and course literature.
- Trends in surveillance and control.
- Affected interests / values.

**2. Course overview and literature**

- What is data protection law?
- Course overview at:  
<[http://www.uio.no/studier/emner/jus/jus/JUS5630/v13/jus5630\\_syllabus\\_2013-1.pdf](http://www.uio.no/studier/emner/jus/jus/JUS5630/v13/jus5630_syllabus_2013-1.pdf)>
- Core literature
  1. Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits* (2002)
  2. compendium of regulatory instruments
  3. selected articles
- Supplementary literature  
Not mandatory; skim-read only; particularly useful for tutorials (latter are primarily for LL.M. students studying ICT Law)
- Useful websites
  1. EU: <[http://ec.europa.eu/justice\\_home/fsj/privacy/index\\_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm)>
  2. Council of Europe: <<http://www.coe.int/t/dghl/standardsetting/DataProtection/>>
  3. Electronic Privacy Information Center (USA): <<http://www.epic.org/>>

**3. Surveillance and control – basic trends**

- Four scenarios:
  1. a prison plan
  2. a war on terror
  3. a war on fraud
  4. a battle for profit
- Principal trend = increasing *mass* surveillance and control (but relative decline in intensity of surveillance and control by *small-scale* groups?)
- Growing pervasiveness along two main axes:
  1. across national boundaries
  2. across organisational sectors
- Cf. Roger Clarke's "surveillance vignettes", at  
<<http://www.anu.edu.au/people/Roger.Clarke/DV/SurvVign.html>>
- Developments in surveillance techniques: Increasingly ...
  - automated
  - de-personalised
  - miniaturised
  - continuous
  - preemptory
  - directed at large groups of people
  - based on transactional and/or biometric data
- Causative factors:
  - Reflexivity (Giddens)

- Rationalisation (Weber)
- Growth in social scale
- Increasing symbiosis between surveillance systems
- Growth in “fine-grained” concern by organisations for their clients
- Wartime exigencies
- Economic significance of information
  - (IRM, data warehousing, data mining, profiling)
- Role of technology (primarily ICT):
  - Double-sided effect of technological developments on privacy (the paradox of technology)
  - Privacy-invasive technologies
  - Privacy-enhancing technologies (PETs)
  - Appeal of ICT:
    - enhance performance efficiency (and *appearance* of efficiency)
    - fascination for the “technically sweet”
- Role of dystopian visions: e.g., ...
  - Orwell’s *1984*
  - Huxley’s *Brave New World*
  - Zamyatin’s *We*
  - Bradbury’s *Fahrenheit 451*
  - Kafka’s *The Trial*
    - Issue: to what extent are these visions realistic and analytically useful?
    - Cf. Foucault’s work on *panopticism*
    - Cf. Anna Funder’s *Stasiland* (2003)

#### 4. Affected interests / values

- Privacy
- Autonomy
- Integrity
- Dignity
- Democracy
- Pluralism

Definitional issues

Privacy as:

- right to be let alone (e.g., Warren & Brandeis)
- informational control / informational self-determination (e.g., Westin)
- limited accessibility (e.g., Gavison, Bygrave)
- solely concerned with intimate sphere (e.g., Wacks, Inness)

Autonomy = self-determination

Integrity = harmonious functionality based on respect

Dignity = intrinsic worth

Democracy = active participation in public government of societal processes

Pluralism =

- diversity of lifestyles and opinions;
- distribution of power so that not one single group/organisation can dominate others

## 5. Catalysts for emergence of data protection law

### 5.1 Technological-organisational trends, particularly as regards data processing

- Growth in amount of data stored
- Integration of these data
  - plans for centralised data registers
  - introduction of PIN systems
  - national census plans
- Increased sharing of data across organisational boundaries
- Growth in re-use and re-purposing of data
- Increased risk of data misapplication
- Information quality problems
  - tendency to ignore quality issues
  - poor “cognitive” quality
- Diminishing role of data subjects in decision making processes affecting them
  - increasing reliance on “digital persona”
  - increasing “anonymisation” of transactions
  - reduction in “cognitive sovereignty”
- Causative factors: see list in section 4
  1. information appetite of organizations
  2. economic significance of information
  3. Appeal of IT
    - enhance performance efficiency (and *appearance* of efficiency)
    - fascination for the “technically sweet”

### 5.2 Public fears

- Two main kinds of fears:
  1. fears over threats to privacy and related values
  2. economic fears
- Three sets of first kind of fear:
  1. Power imbalance
  2. Loss of control over technology
  3. Dehumanisation
- First kind of fears nourished by:
  - trauma of fascist oppression
  - Watergate
  - dystopian visions
  - certain types of IT (mainframe computers)
  - increased risk consciousness (Beck)Cf. Surveys of public attitudes to privacy
  - what do these tell us?
- Second main kind of fear:
  - focuses upon potential for restricting TBDF and thereby trade in goods and services
  - manifest in *international* instruments, particularly OECD Guidelines, EC Directive on data protection, APEC Privacy FrameworkCf. Data protection laws as instruments for economic protectionism?
  - Lack of solid evidence

### 5.3 Legal factors

- Positive legal factors
  - international human rights, especially right to privacy

- Art 12 UDHR, Art 17 ICCPR, Art 8 ECHR
- rights in national constitutions
  - See especially German Federal Constitutional Court – Census Act decision of 1983; Hungarian Constitutional Court – PIN decision of 1991
- administrative law; doctrines on rule of law
- right to privacy/personality in statute and case law
  - See, e.g., Norwegian Supreme Court decision of 1952 on film screening; US case law
- rules on defamation, discrimination, intellectual property, fair labour practices
- role of property doctrines?
- role of FOI law?
- Negative legal factors:
  - pre-existing rules found insufficient
  - pre-existing rules sometimes privacy-threatening
    - E.g., Swedish tradition of open government / FOI
- Cf. cross-fertilisation process
  - development of data protection guarantees in international human rights law
  - EU recognition of data protection as fundamental right in itself