

Re-Inventing Data Protection?

Brussels 12-13 October 2007

Technical Standards as a Form of Data Protection Regulation

Jane K. Winn

University of Washington

School of Law

Technical Standards as Data Protection Regulation

- Regulatory Pluralism and Meta-Regulation
- Technical Standards and Regulation
- ICT Standards Are Not Product Standards
- Nor Are Adaptive Management Standards
- ICT Standards as Regulation
 - US and EU approaches
 - Successes and failures
- Conclusion
 - ICT standards for economic and social goals
 - Meta-regulation as better regulation?

Regulatory Pluralism & Meta-Regulation

- Anglo-Australian School of Regulatory Studies
 - Compare: EU New Modes of Governance
- Regulatory Pluralism
 - Public Law
 - Private Law
 - Soft Law
 - Self-Regulation
 - Social Norms
 - Technical Standards
- Meta-Regulation
 - Constrain Regulatory Pluralism/Regulate Self-Regulation

Technical Standards and Regulation

- Industrialization spawned modern standards; globalization fuels increasing demand
 - Lower production, transaction costs
 - Increase producer competition
- Trade subject to technical standards
 - World trade: 80% world trade; Intra-EU trade: 76%
- Voluntary Standards to Complement Regulation
 - Mandatory standards: rent-seeking; obsolescence
 - WTO Technical Barriers to Trade Agreement
 - EU New Approach to standardisation
 - Global consensus among regulatory capitalist economies
 - US Market-led approach
 - Exceptional reliance on private, voluntary, consensus, redundant processes

ICT Standards Are Not Product Standards

- **Product Standards for Industrial Economy**

- *De jure* international: ISO
- *De jure* EU: CEN
- *De jure* national: NSBs (BSI, DIN, AFNOR)
- US Federation of Private SDOs: ANSI
 - Transparency and openness [Due Process]

- **ICT Standards for Information Economy**

- *De jure* international: IEC, ITU
- *De jure* EU: CENELEC, ETSI
- International de facto: IETF, W3C, OASIS
 - Transparency and openness?
- Consortia: private and effective
- Proprietary technologies

Adaptive Management Standards Are Not Product Standards

- ISO 9000
 - Quality Management Systems
- ISO 14000
 - Environmental Management Systems
- ISO 26000
 - Social Responsibility Management Systems
- ISO 17799/27000
 - Information System Security Management Systems
- ISO 31000
 - Risk Management System Standards

Defining Global Information Architecture

- Consortia and de facto international ICT SDOs move quickly
 - Standardize minimum
 - Defer consideration of social issues
- Logic of Collective Action
 - single minded small groups out-maneuver divided big groups
- “In the beginning, all the world was America, and more so than that is now...” John Locke
 - Institutional Isomorphism: unregulated global markets resemble deregulated US markets

“New Approach” for ICT?

- New Approach: Standards in support of regulation/co-regulation
- Electronic Signatures
 - But no significant private sector adoption
- Data Protection
 - Commission mandate to CEN blocked by industry opposition
- Other examples?

Reinvent EU ICT Standards Policy?

- Lisbon Agenda: Leverage European Innovation
- Integrate ICT standards policies among different DGs
- Broad dialogue among regulators and stakeholders
 - Support standards from consortia with WTO transparency and openness
 - Balance public interests and private IPR
- Watch this space: RFID; e-Invoicing; SEPA

US Failure & Success

- Platform for Privacy Preferences P3P
 - Limited scope, limited support from privacy advocates or industry
 - Result: Irrelevance?
- Adaptive Management Standards
 - Sarbanes-Oxley: ISO 17799/27001
 - HIPAA Security Standard: federal regulation
 - Gramm-Leach-Bliley Safeguards Rule: federal regulation
 - Federal Trade Commission Consent Orders
 - ISO 17799/27001
- Payment Card Industry Data Security Standard
PCI/DSS
 - <https://www.pcisecuritystandards.org/>
 - “Enforced self-regulation” based on consensus industry standards
 - October 1, 2007 deadline for compliance

Conclusion

- ICT Standards for Efficiency: Information Security
 - US consortia model for ICT technologies
 - Private enforced self-regulation: PCI/DSS
- Adaptive Management Standard for Data Protection
 - CEN/ISSS Workshop on Data Protection Best Practices
- ICT Standards for Social Goals: Data Protection
 - Greater coercion required for health/safety/social justice goals than efficiency
- Meta-Regulation as Better Regulation?
 - Unambiguous mandate ex ante
 - Ex post review of substance of self-regulation
 - Escalating public enforcement