

PRIVACY HORIZONS: TERRA INCOGNITA

29th International Conference of
Data Protection and Privacy Commissioners

September 25 to 28, 2007
Montreal, Canada



LES HORIZONS DE LA PROTECTION DE LA VIE PRIVÉE : TERRA INCOGNITA

29^e Conférence internationale des commissaires
à la protection des données et de la vie privée

du 25 au 28 septembre 2007
Montréal, Canada

‘Saying what you do and doing what you say’: Arguments and Prospects for an International Privacy Standard

Colin J. Bennett

Department of Political Science

University of Victoria, BC.

cjb@uvic.ca

Robin Bayley

Linden Consulting Inc. Victoria, BC.

rmbayley@shaw.ca

Why organizations registered to ISO 9001 should have better personal information management

- Awareness of their operating systems and personal data holdings
- Staff training
- Must think through and address regulatory requirements
- Ability to capitalize on outside expertise, through conformity assessment process

Requirements of a Privacy Management Standard

- Translation of Fair Information Principles into language and format of standards
- Provision of guidance for implementing the principles in organizations
- Appropriate conformity assessment tools for business size and data sensitivity
- Audit guide
- Accreditation system for privacy auditors

Overlap between quality management and data protection

- Transparency of policy and purpose
- Procedures for interaction with data subjects
 - Complaints resolution
 - Access and correction requests
 - Consent provision and withdrawal
- Personal data management procedures
 - Data security
 - Data quality
 - Data retention

Motivations for adoption of privacy standards

- Through Educational and Regulatory Powers of Data Protection Authorities
- Through Desire for Competitive Advantage
- Through Referencing the Standard in Contracts

Initiatives for Privacy Management Standardization

- National Standards Bodies
 - Canadian Standards Association (CSA)
 - American National Standards Institute (ANSI)
- International Standardization Organization (ISO)
 - Work of JTC-1 of ISO and International Electro-Technical Commission (IEC)
- European Committee for Standardization/Information Society Standardization System (CEN/ISSS)
- International Security, Trust, and Privacy Alliance (ISTPA).